2023-2030

Australian Cyber Security Strategy Discussion Paper

JANELLIS AUSTRALIA SUBMISSION

Janellis

LETTER OF THANKS

Dear Home Affairs and the Cyber Strategy Task Force,

Thank you for the opportunity to contribute our perspective towards the task of shaping Australia's cyber security strategy.

Janellis Australia has worked with leading organisations and government agencies to build their resilience since 2006. Many of the organisations we work with are owners and operators of critical infrastructure and operate in high-risk industries.

The current cyber security threats are described as the biggest crisis facing Australian organisations in recent times. Yet this type of threat is not new. Since 2000, Australian organisations have faced the threat of terrorism, targeting businesses and critical infrastructure providers. Our submission draws upon the lessons learnt from previous risks Australia has faced and successfully responded to.

In our experience in building organisational resilience within critical infrastructure industries, the most robust method of preventing privacy breaches and building cyber resilience requires a multi-faceted approach that includes government and business working together.

We believe that the Australian government should aim to build cyber resilience, rather than cyber security and guide all organisations to implement strategies to uplift their cyber resilience. Leaders can draw upon the experiences of organisations who have developed a mature capability to respond to a range of potential threats.

Key elements to building cyber resilience include:

1. Taking an "all-risks" approach to building resilience.

2. Embedding a decision-making framework to enable critical thinking to occur.

3. Conducting robust scenario-based activities for all types of risks, to uncover vulnerabilities and uplift capability.

4. Utilising a cyber resilience scorecard.

The evolving nature, potential severity and velocity of cyber risks has brought cyber security into sharper focus, yet cyber risk is just one operational risk that organisations are managing. Investments in cyber risk management need to draw upon existing risk management practices to develop the capability to respond to all risks and emerging threats, such as third-party risks.

Cyber specialists say human error is still the cause of 99% of cyber breaches and yet there is a predominant focus on improving the technology aspects of cyber security rather than the human aspects. This imbalance leaves organisations vulnerable. To combat the ever-present threat of cyber-criminal activity, organisations need to uplift and embed critical thinking skills and ensure that high-quality, robust, transparent, discoverable, and defendable decision-making is occurring at all levels of the organisation. Scenario-based exercising activities can be used to uncover blind spots and vulnerabilities and uplift critical thinking skills. An Organisational Resilience or Cyber Resilience Scorecard can assess and maintain capability and provide assurance to key stakeholders.

Based on our extensive experience in helping organisations become more resilient, we share our recommendations in this submission.

Best regards,

Natalie Botha
Managing Director

CONTENTS

2023–2030
AUSTRALIAN CYBER SECURITY STRATEGY

JANELLIS AUSTRALIA SUBMISSION

1. WHAT IDEAS WOULD YOU LIKE TO SEE INCLUDED IN THE STRATEGY TO MAKE AUSTRALIA THE MOST CYBER SECURE NATION IN THE WORLD BY 2030?

The Australian government can achieve higher levels of assurance organisations can prevent and rapidly respond to major and multiple cyber-attacks, by guiding organisations on 'better practice' ways to build their cyber resilience.

The current cyber security threats are described as the biggest crisis facing Australian organisations in recent times. However, in mid-2000, Australian organisations were similarly facing the threat of terrorism, targeted at our business community and critical infrastructure providers. In our experience in helping large and complex organisations build resilience within critical infrastructure for more than 15 years, we found a multi-faceted approach builds cyber resilience. The aim of this submission is to share the key elements that can be used to guide organisations on how to build their cyber resilience.

Recommendation 1:

Draw upon the lessons learnt from responding to previous significant risks

In early 2000, Australian leaders faced significant risks that were targeted at critical infrastructure providers and organisations operating in high-risk industries. To help leaders understand the challenges and find ways to work together to solve them, Janellis convened an industry conference which engaged more than 200 participants from private enterprise, critical infrastructure providers, government agencies and emergency services. We designed and explored a Hypothetical Scenario of an event occurring in the Sydney CBD, which included the IAG Crisis Management Team and agency representatives sharing their response, on a panel, in front of a live audience and the media.

Former Chief of the Australian Defence Force, Sir Peter Cosgrove facilitated the landmark day, and commented at the time:

"Australia has some of the best men and women leaders of any country in the world who can deal with business shocks standing on their feet and they have already demonstrated this. However, the new set of challenges needs more work. Some organisations are very advanced and responsible—and there are a lot who are not. In running through the hypothetical today, we can start to imagine the dimensions to the problem."

Since then, critical infrastructure organisations operating in high-risk industries have worked with the Federal Government to build their resilience capability to apply these lessons learnt to withstand threats of this magnitude. In our view, the approach to the new cyber security risks should take the same approach.

Recommendation 2:

Encourage organisations to improve how they anticipate, detect, manage and recover from cyber attacks

Based on the lessons learnt from the past, many organisations operating in high-risk industries use an Organisational Resilience Framework that fuses the disciplines of risk management, with readiness planning, response capability and assurance. ***See Appendix 1.***

Organisations with a mature capability have used ***four key strategies, which have provided enduring value:***

1. Taking an "all-risks" approach to building resilience.
2. Embedding a decision-making framework to enable critical thinking to occur.
3. Conducting robust scenario-based exercising for all types of risks, to uncover vulnerabilities and uplift capability.
4. Implementing a resilience scorecard that includes cyber risks.

Whilst meeting the regulator's expectations is a key factor in designing resilience capability, the overarching focus should be to build the capability to withstand any threat an organisation may face, and this in turn will satisfy the regulators.

In working with Sir Peter Cosgrove, Janellis developed a Decision Support Tool that draws upon the rigor of military decision-making principles but designed specifically for business leaders. Janellis trained executive teams operating in Australia, USA, Canada and India by applying the framework to scenarios designed for their regional risks and operating context.

For example, Janellis embedded the Decision Support Tool within a leading airline as part of a broader resilience program. This involved identifying high priority individuals and teams responsible for complex and high-impact decisions and providing learning opportunities to apply a critical thinking framework within scenario-based exercising activities. The framework enabled team-based critical thinking to occur within and across teams.

In the Financial Review article 'Seven Steps to Dealing with the COVID-19 Crisis', Peter Durkin wrote:

"As business leaders come to grips with the impacts of COVID, a methodical decision-making process has never been more important."

Natalie Botha said, *"An effective decision-making process could help prevent fatal mistakes."*

John, who had a pivotal role in maintaining Organisational Resilience at a leading airline has said:

"An organisation may have a clear strategy, exhaustive risk management processes, detailed plans and highly skilled individuals but if teams come together and are unable to demonstrate 'critical thinking', they may not be effective in managing the situation or seeing the opportunities."

Recommendation 3:
Encourage organisations to build cyber resilience across the enterprise and include third party providers

In a study that investigated Australia's preparedness for cyberattacks, Cisco found that 92 per cent of Australian businesses expect a cybersecurity incident to disrupt their business in the next 12 to 24 months.[2] IBM also found the average total cost of a data breach is US$4.35 million.[3]

According to Cybersecurity Ventures, protecting consumers from cybercrime will drive global spending on cybersecurity services to $1.75 trillion for the five-year period from 2021 to 2025.[4] It's clear, organisations are spending a significant amount on continuing to secure their systems.

Yet the government's Australian Cyber Security Centre's (ACSC) guidelines for preparing and responding to cyber security incidents *predominantly focus on improving the technology aspects of cyber security.*[5] Similarly, in the US, most organisations evaluate their cyber maturity according to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, *but it is 80% focused on identification, protection, and detection, and only 20% on an organisation's ability to respond to and recover from a breach.*[6] This imbalance leaves organisations vulnerable.

Although teams and executives complete ongoing cyber awareness training, cyber specialists say human error is still the cause of 99% of cyber breaches.[7] In addition to the current guidelines and investments in protecting the data, the focus needs to include the human dimension of cyber resilience.

It is estimated that approximately 90 per cent of cyber breaches begin with a successful phishing attack,[8] which today can access critical data within an average of 72 minutes,[9] however, IBM found it takes an average of 277 days for organisations to identify and contain the attack.[10]

The increasingly complex and interconnected operating environment requires cyber risks related to third parties to be managed more effectively. A mature cyber risk management culture extends the focus to understanding the risks and vulnerabilities of critical suppliers and other third parties.

What more can organisations do?

To prevent cyber security breaches, organisations need to improve how they anticipate, detect, manage and recover from cyber-attacks.

Cisco's 2023 Cybersecurity Readiness Index found that only 15 per cent of organisations globally possessed a level of cybersecurity preparedness mature enough to handle cyber security risks.

However, in Australia, that figure is only 11 per cent. Almost 90 per cent of Australian companies are yet to fully implement a robust cyber security system.[11]

While not all cyber-attacks can be prevented, their impacts can be minimised through better preparation.[12] Studies show although organisations can expect ongoing cyber threats and risks, how they respond is critical, as the same threat can result in very different impacts based on an organisation's degree of preparedness,[13] otherwise known as cyber resilience.

What is Cyber Resilience?

Cyber Resilience is a holistic and cross-functional approach to anticipating, detecting, managing and recovering from cyber security incidents while maintaining continuous business operations. It encompasses uplifting the critical thinking skills of the organisation to identify, mitigate and respond effectively to all cyber security risks.

A mature cyber resilience capability requires a holistic and cross-functional approach which is demonstrated by:

- An enterprise-wide view of all cyber-related risks and emerging threats, that are managed alongside other business risks including strategic, operations, people, financial, market, political, environmental and reputation.

- Joint planning and a co-ordinated response between executive leaders, cyber response, business incident management and crisis management teams.
- A multi-faceted approach that supports technical measures with frameworks and aligns with best practices, industry regulations and standards.
- High levels of confidence to respond to cyber-related emerging threats through scenario-based exercising and training activities.
- Addressing the human elements of cyber resilience by developing critical thinking skills at all levels of the organisation so teams can uncover vulnerabilities, identify blind spots, gaps in capability and respond to cyber incidents successfully.
- Aligning cyber resilience capability with key third-party providers.
- Regular assurance to the board and other key stakeholders.
- A faster recovery which helps mitigate financial, reputation and data loss.

Recommendation 4:
Encourage organisations to implement a cyber resilience scorecard

A Cyber Resilience Scorecard and 'better practice' resilience tools and framework enable organisations to assess and build cyber resilience capability. A scorecard can be used to identify areas that need immediate action, validate investments and provide assurance to internal and external stakeholders.[14]

The scorecard reviews current investments and competencies against recognised standards and provides tools and recommendations for implementing and maintaining resilience across the organisation.

The cyber resilience scorecard should be aligned with NIST Cybersecurity Framework, ISO/IEC 27001 Information Security Management, industry specific standards and board level guidelines including AICD Cyber Security Governance Principles.

Key elements of the Janellis Cyber Resilience Scorecard are aligned with the Janellis Organisational Resilience Framework, which fuses cyber resilience capabilities within a single framework that includes Risk, Readiness, Response and Assurance. ***See Appendix 1 for details.***

The scorecard helps organisations:

- Validate and prioritise cyber resilience investments.
- Identify gaps in design or capability that need immediate action.
- Determine areas of excellence that should be applied more broadly.
- Ensure adequate insurance cover and third-party support.
- Provide a cyber resilience capability uplift roadmap.
- Provide assurance to key stakeholders internally and externally.

To learn more, visit:
www.janellis.com.au/cyber-resilience-scorecard

Recommendation 5:
Encourage organisations to conduct regular scenario exercising activities

According to the AICD's Cyber Governance Principles, scenario exercises and testing are a key part of a cyber incident response plan to prepare directors, and the broader organisation, as well as third party providers to respond effectively to a significant cyber incident. Scenarios enable directors to become familiar with their oversight responsibilities and identify areas for improvement while working through the scenario with management and experts.[15]

Responding effectively to cyberattacks also requires a collaborative approach. When IT or cyber departments function as separate entities from risk management, research shows they are more likely to experience an attack.[16]

Building enterprise-wide cyber resilience involves an ongoing program of scenario-based training and exercising across various levels of the organisation.

Using a 4-Step Exercise Development Process to develop scenarios and train executives and management teams can establish an effective cyber resilience culture. With support from top management, regularly training and exercising cyber scenarios across teams develops relationships and an understanding of roles and responsibilities that will be crucial during a live incident.[17]

Cyber scenario-based planning helps decision-makers anticipate change, prepare responses and create more robust strategies[18 19]

By considering a range of possible cyber risks and threats in the context of emerging trends, environmental change and driving forces, decisions are better informed and strategy based on deeper insights is more likely to succeed. Exercising is the optimal way to learn critical thinking as it provides teams with a real time, dynamic and immersive experience using a complex scenario. When anticipated in advance, the impacts of risks and vulnerabilities can be avoided or reduced more effectively than during a crisis incident.

Scenario-based exercising and training enables teams to jointly analyse potential cyber threats or vulnerabilities and their impacts and develop approaches to mitigate them. Organisations that undertake regular exercising with senior management and teams have been shown to reduce incident response times significantly.[20] In fact, breaches at organisations with Incident Response (IR) teams that regularly test their plan saw US$2.66 million in savings compared to breaches at organisations with no IR team or testing of the IR plan.[21] Organisations can respond quickly to contain the fallout from a breach by establishing a detailed cyber incident playbook and routinely test that plan through tabletop exercises or scenario exercising in a simulated environment.

This approach delivers competitive advantage and provides assurance to key stakeholders that organisations can respond effectively to cyber threats and minimise financial, reputational and data loss as well as operational disruption.

Use a robust Scenario Development Process

A robust scenario development process should draw upon the expertise within the business and leverage existing investments and capability. The process should be used to develop credible scenarios that uplift and embed capability.

STEP 1—SCOPE

The scoping phase establishes the critical drivers for the activity; identifies the key stakeholders; ascertains current capability and determines the gaps to be addressed or highlighted, and confirms the key objectives.

STEP 2—DESIGN

The design phase involves identifying the scenario and ensuring it is current, relevant and will challenge and build capability. The chosen scenario should build on previous scenarios or exercise activities to engage new stakeholders.

STEP 3—FACILITATE

Successful delivery is the result of expert facilitation skills that manage both the pace and outcomes of the activity, ensuring participants are engaged and confident during the exercise.

STEP 4—REPORT

The final phase involves evaluating the exercise feedback and providing recommendations in a report to resolve areas of vulnerability and highlight areas of excellence.

Studies show although organisations can expect ongoing cyber threats and risks, how they respond is critical, as the same threat can result in very different impacts based on an organisation's degree of preparedness.[22] Scenario-planning helps teams understand their environment, share knowledge, consider the future and assess strategic options.

Scenarios enable teams to simulate a range of potential cyber risks or threats, to test and evaluate decision-making, actions and plans.

This planning process creates awareness of vulnerabilities and improves decision-making,[23] which mitigates financial, reputation and data loss.

Example: Paul from Westpac who is responsible for the enterprise-wide exercising program says:

"Westpac executives come together in a closed loop learning environment—that may include business partners—in a way that allows them to have engaging, open and robust discussions. Using a series of scenarios they can challenge preconceptions and uncover blind spots. The outcome of these activities is always a deeper understanding by our business of the challenges and opportunities that we face from a broad group of stakeholders.

The Westpac tools provided to the teams are used across the organisation internationally at all levels—and aim to enhance the critical thinking capabilities as an ongoing investment into building the organisation's resilience."

Recommendation 6:
Encourage organisations to embed a decision-making framework across the organisation

In the event of a major cyber-attack, the challenge for the executive team is to make rapid, critical decisions that impact customers and shareholders with limited information. Considering a ransom demand is a complex decision-making process and probably one of the most difficult decisions that a board will encounter.

We could argue that boards and executives make complex decisions every day and that most would possess an intuitive capability. The challenge with this type of decision, compared to others the board would make, are the higher levels of scrutiny and uncertainty and significant, potential, cascading impacts in the short and long term. Cyber security related decisions also have evolving technical complexity, conflicting or incomplete information and many competing stakeholders' needs and expectations to consider; and the decision needs to be transparent and defendable.

Currently, few organisations have an agreed, unified, robust, and transparent decision-making framework that can address this level of complexity; and even less have a unified decision-making framework embedded across the enterprise to manage internal events such as security errors that enable cyber-attacks to occur.

Arguably, these are the blind spots and vulnerabilities that cyber criminals seek to exploit.

Recommendation 7:
Encourage organisations to build and demonstrate critical thinking skills across the organisation

To combat the ever-present threat of cyber-criminal activity, organisations need to *build and demonstrate strong critical thinking skills at every level from the individual to the team, executive leadership teams, all the way up to the board*.

Resilient organisations ensure robust and high-quality decision-making is occurring at all levels of the organisation in the key resilience areas of risk, readiness and response.

Cyber resilience decisions require complex decision-making skills, due to evolving technical complexity, conflicting or incomplete information and many competing stakeholders' needs and expectations.

Other factors which contribute to the complexity of cyber resilience decisions are:

- High levels of scrutiny, increased pressure from the regulators, greater demands for transparency and evidence of a robust, discoverable, and defendable decision-making process.
- Compressed timeframes, social media, mainstream media and community expectations are driving the timeframes for decisions, even where there may be incomplete or inconsistent information.
- Significant impacts where a single poor decision or an accumulation of poor decisions can result in cascading impacts.

Examples of cyber-related decisions with significant impacts include the decision to click on a phishing email, or more complex decisions such as those related to investments in critical third-party systems and strategies to build and maintain cyber resilience capability.

All these decisions require critical thinking and high-quality decision-making. This is especially important now as cyber criminals are becoming more professionalised, industrialised, powerful and effective.[24] They demonstrate strong critical thinking capabilities in locating weaknesses within the organisations they are targeting, and executives such as Coles Group Chief Executive Steven Cain have observed their attacks are becoming more sophisticated.[25] To reduce their vulnerability to cyber-attacks, organisations need to demonstrate at least similar, or higher levels of critical thinking within the business as that which is occurring outside of the business.

The lack of a transparent decision-making framework at any layer of most organisations suggests that high-quality decision-making is not considered a business-critical capability that needs to occur daily at every level of the organisation. Many organisations have enterprise-wide systems and risk management frameworks, but they lack a consistent and transparent decision-making process for use across the enterprise.

A robust decision-making framework enables critical thinking skills by ensuring individuals and teams take the time to apply best practice tools to separate facts from assumptions, uncover bias and blind spots, identify the main issues or risks, consider potential scenarios, and the broader impacts before making decisions.

Most cyber-attacks succeed usually, not because of complex methods used by criminals, but, rather, because of the difficulty in establishing an effective cyber resilience culture.[26]

To achieve higher levels of assurance that teams can prevent and rapidly respond to major and multiple cyber-attacks, organisations can embed Critical Thinking across the enterprise.

A Critical Thinking Framework and the Critical Thinking Accreditation Program can upskill individuals and teams to:

- Identify, anticipate, detect and manage threats.
- Consider potential scenarios and uncover blind spots.
- Recognise, escalate and respond to incidents more quickly.
- Make rapid and effective decisions with incomplete or conflicting information, high levels of scrutiny, compressed timeframes and significant impacts.

Creating a culture of cyber resilience across the organisation involves improving how teams assess cyber threats and breaches by building resilience and an adaptive capacity to respond:

- Review all current cyber security guidelines, standards, and legislation relevant to your organisation.
- Elevate 'high-quality decision-making' to business critical and gain endorsement at the executive and board level to embed a standardised, best practice approach to decision-making across the organisation.
- Implement a Cyber Resilience Scorecard and a Cyber Resilience Benchmarking Framework to assess and build capability across the organisation.
- Identify a Critical Thinking Framework that can be used at all levels of the organisation to review and build capability to respond to cyber security risks. The Critical Thinking Framework needs to be used in risk identification, mitigation, and response by individuals for high-quality 'in the moment' rapid decision-making, as well as by teams to work through more complex problem-solving and decision-making.
- Review your current Cyber Resilience capability against the guidelines and legislation to generate a shared view of current high priority risks and immediate actions. Ensure the review includes your broader resilience capability, such as enterprise risk management, business continuity, disaster recovery and incident and crisis management.
- Complete War Room Scenario Planning activities using the Critical Thinking Framework to uncover blind spots, resolve immediate areas of vulnerability and build capability.
- Identify people within the organisation and subject matter experts who have strong decision-making/critical thinking skills to facilitate social learning opportunities, model high-quality decision-making, and accelerate the capability uplift.
- Identify all high priority teams responsible for preventing or responding to cyber threats and develop a capability uplift program that embeds high-quality decision-making and critical thinking within these teams.
- Develop an enterprise-wide Critical Thinking Capability Uplift Program to ensure individuals and teams have the skills to identify, anticipate, detect, manage, respond, and recover from on-going cyber related risks. Embed the capability through the Critical Thinking Accreditation Program that includes scenario-based planning, social learning opportunities, access to tools, templates, eLearning and aide memoires to build, consolidate and maintain high-quality decision-making capability.

2. COMPANY DIRECTORS ADDRESSING CYBER SECURITY RISKS AND CONSEQUENCES

Many company directors and executives are navigating uncharted waters in responding to the increased threats and impacts of cyber security risks and those related to third-party providers.

In our view, company directors should be held accountable for addressing cyber security risks and managing their consequences. According to the World Economic Forum's Principles for Board Governance of Cyber Risk company directors and business leaders need to:

- Incorporate cybersecurity expertise into board governance.
- Encourage systemic resilience and collaboration.[27]

The challenge for company directors, and all teams responding to a crisis is that they're often required to make high-quality decisions with limited warning, conflicting or incomplete information, technical complexity, high levels of scrutiny, compressed timeframes and with significant community expectations for effective communications.

The ability to come together with little notice and make high quality decisions with incomplete or conflicting information, relies on critical thinking skills, broadly classified as the ability to cut through different types of information, problem solve and prioritise actions.

Company directors and senior leaders have typically honed these skills through experience and apply them intuitively to any situation. The temptation during a crisis is for the company director to use these skills to lead the organisation out of the crisis.

The difficulty with this approach is that the role of leading a crisis and becoming the key spokesperson are both critical roles and company directors who attempt to do both may compromise the effectiveness of the overall response.

What can company directors do to prepare for an optimal crisis response?

Organisations can prepare for crisis events through scenario-based exercising activities which are used as a closed-loop learning opportunity to identify vulnerabilities, blind spots, catastrophic risks and build capability. Leaders should avoid choosing scenarios that are easy and where they believe they have adequate controls and instead consider 'worst case scenarios' where all the controls have failed and build a capability for these types of catastrophic risks.

During the scenario activity the team should focus on using tools and processes that can be applied to any scenario to gain clarity on roles and responsibilities. These tools should include a decision-making framework that enables team-based critical thinking. Decisions during a crisis need to be robust, transparent, discoverable, and defendable.

Using a series of scenarios, teams can challenge preconceptions, uncover blind spots and build a common operating picture that will allow them to challenge their thinking.

A wide range of people should be trained on the tools and there should be no single person responsible for an incident or crisis. Several people need to be able to lead the crisis and a few people need the capability to assume the role of media spokesperson. This will be important if the crisis event requires the ongoing communication of facts and information as it unfolds.

The outcome of these activities is a deeper understanding of the risks the organisation faces and an opportunity to build capability to respond to those risks prior to a crisis occurring.

"Company directors need to be clear on their role in a crisis and ensure that high-quality decision-making that is transparent; robust; discoverable and defendable, is occurring within the activated response teams."

The company director's main role, prior to a crisis occurring, is ensuring the organisation is effectively prepared to respond to a range of risks, threats and disruptive events.

The company director needs to ensure that:

- Emerging risks are monitored effectively, and contingency plans are developed for significant emerging threats, as they are identified.
- The organisation has the demonstrated capability to respond to a range of strategic, operational, financial, and environmental threats.
- There is a robust and strategic exercising program with scenario-based activities to develop critical thinking capabilities at multiple levels within the organisation including the incident, emergency and crisis level.
- The organisation has access to crisis, emergency and incident management tools to enable them to respond in a coordinated way that facilitates critical thinking.
- Members of the executive team understand how the organisation would respond to a crisis event, including key roles and responsibilities.

During a crisis, the company director may be required to:

- Become a 'sounding board' to the crisis management team for significant strategic decisions that need to be made. This may be crucial to the effectiveness of the crisis chair and the crisis management team, depending on the size, complexity and scale of the crisis.
- Challenge and endorse the key strategic decisions and actions of the crisis management team and provide board level communications regarding these key decisions.
- Enter into the decision-making process and make decisions with the crisis management team where there may be incomplete or conflicting information and significant impacts.
- Liaise with key external stakeholders including the regulators, shareholders and the media, only as agreed by the crisis management communications team.

Assurance needs to be provided to the company director so they trust in the capabilities of the executive leadership team and the crisis management team. Members of the board need to be confident the crisis management team can manage the strategic requirements of a crisis.

Clear expectations are critical in this relationship

The crisis management team needs to understand before the crisis event, what the company director requires during the crisis response, and how they will support the associated organisational response. Conversely, the company director needs to understand the needs of the executive leadership team during a crisis.

Company directors should resist the urge to make too many demands on management's time during a crisis. The crisis management team members should have established relationships and processes and be best placed to understand the impacts across the organisation and to mobilise the appropriate resources.

An effective crisis management team should provide assurance and demonstrate critical thinking capabilities by: separating facts and assumptions; identifying what is unknown; understanding the impacts across the organisation; considering most likely outcomes and worst case scenarios; identifying key stakeholders impacted and developing and communicating critical decisions.

This process will often take place with incomplete information and under immense time pressure. The crisis management team will ideally focus on managing the crisis rather than managing the board requirements.

In what situations would the board need to operate as a crisis team?

The role of the board may change from a role of oversight to one of leadership where the crisis has a direct impact on the chief executive and/or their leadership team. Questions board members should be asking at this time are:

1. Are any members of the crisis management team implicated or impacted by the crisis?
2. Does the crisis management team have the skills and capability required to respond to this event?
3. Does the crisis management team need additional support?

If the entire crisis management team and their alternates are unable to lead a crisis, the strategic decisions will lie with the board, and they will need to assemble and direct a new crisis management team.

What can the company director do to prepare for a crisis event?

Company directors have a highly influential role in crisis management preparedness. They should be asking executive leaders targeted questions to ensure that an adequate level of preparedness has occurred, and that capability exists at all levels within the organisation.

Responding to cyber security threats

Many company directors and executives are navigating uncharted waters in responding to the increased threats and impacts of cyber security risks. The evolving nature, potential severity and velocity of cyber risks require organisations to take a more targeted and focused approach to assess, build and maintain cyber resilience capability.

Company directors can uplift cyber resilience capability by:

- Implementing a Cyber Resilience Framework that incorporates key areas such as Risk, Readiness, Response and Assurance.
- Utilising a Cyber Resilience Scorecard to identify gaps that need immediate attention, areas of excellence to be applied more broadly and provide assurance to key stakeholders.
- Elevating high-quality and transparent decision-making to 'business critical' and identifying a Critical Thinking Framework that can be used at all levels of the organisation to review and build capability and provide assurance.
- Facilitating board and executive level discussions on complex or technical cyber security decisions, such as paying a ransom and reaching consensus on the way in which decisions will be made, utilising a transparent and defendable decision-making process.
- Conducting board or executive War Rooms to create awareness, uncover areas of concern or build assurance for cyber security events.

How can company directors support 'better practice' in crisis management?

Better practice crisis management is evident when critical thinking and high-quality decision-making are occurring at all levels of the organisation in the prevention, preparation, and response to a crisis.

Company directors should ensure their organisations have a transparent and robust decision-making process and that decisions reached are both discoverable and defendable. A pre-defined and consistent decision-making framework will allow crisis management team members to seamlessly enter the decision-making process, as required, drawing upon their diverse expertise.

Organisations with high levels of trust between board members and the executive team can work together to build and maintain a mature cyber resilience capability.

Summary

Company directors have a highly influential role in crisis management readiness. Their role is critical in ensuring emerging risks are monitored effectively and contingency plans are developed for significant emerging threats, as they are identified. They also need to ensure the organisation has the demonstrated capability to respond to a range of strategic, operational, financial, and environmental threats. The primary way to do this is by implementing a robust and strategic exercising program to develop critical thinking capabilities at multiple levels within the organisation including the incident, emergency and crisis level.

3. WHAT WOULD AN EFFECTIVE POST-INCIDENT REVIEW AND CONSEQUENCE MANAGEMENT MODEL WITH INDUSTRY INVOLVE?

An effective Post Incident Review (PIR) model includes a robust 4-Step Process that all organisations can apply to all incidents. The PIR should be used to evaluate an organisation's response to a disruption, threat or incident and the PIR can be designed to focus on a specific set of stakeholders or processes or it can include every facet of the response and involve external stakeholders.

The PIR process should be designed to:

- Assess response effectiveness.
- Provide recommendations to address immediate areas of concern.
- Benchmark an organisation's response against 'better practice'.
- Provide recommendations to uplift and improve capability.

Post-Incident Reviews help build organisational resilience by:

- Enabling teams to take pre-emptive steps to ensure they can manage future threats and risks and mitigate reputation, data and financial loss.
- Providing assurance to key stakeholders that organisations can respond effectively to incidents and minimise disruption.
- Providing a comprehensive report that benchmarks the organisation's response against 'better practice' and includes detailed recommendations to uplift capability.

Post Incident Reviews provide organisations with significant learning opportunities by identifying strengths and weaknesses to enhance and build organisational resilience following a crisis, incident or emergency.

4. WHAT MORE CAN GOVERNMENT DO TO SUPPORT AUSTRALIA'S CYBER SECURITY WORKFORCE?

The World Economic Forum's Global Cybersecurity Outlook Report found 59% of business leaders and 64% of cyber leaders ranked talent recruitment and retention as a key challenge in managing cyber resilience. Additionally, less than half of respondents reported having the people and skills needed today to respond to cyberattacks. Once hired, organisations can train professionals to become effective cyber employees. Technology can always be taught, but traits such as curiosity, problem-solving and critical thinking are vital for cyber professionals.[28]

With today's shortage of available cyber resilience professionals, managing cyber resilience depends on upskilling broader business teams with effective cyber specialist skills. Uplifting capability across the organisation in problem-solving and critical thinking skills is vital in building cyber resilience.

A Cyber Resilience Professional Accreditation Program provides professionals with the opportunity to learn how to apply the Cyber Resilience Scorecard to enable a more strategic and holistic approach to enhancing cyber resilience within their organisation.

Summary

Organisations today are tackling multiple, major cyber security breaches using technology solutions alone, which continues to comprise their customers' privacy and personal safety, all the while incurring millions of dollars in fines along with data, reputation and financial losses.

Building sustainable cyber security across Australia requires thinking more holistically, drawing upon lessons learnt from previous industry responses to risks and building cyber resilience. Cyber resilience is a holistic and cross-functional approach to anticipating, detecting and managing and recovering from cyber security incidents while maintaining business operations. It requires using a Cyber Resilience Scorecard to assess capability, embedding an enterprise-wide cyber resilience response framework and conducting regular scenario-based planning, exercising and training. It encompasses uplifting the critical thinking skills of the organisation to identify, mitigate and respond effectively to all cyber security risks.

Company directors have a highly influential role in crisis management readiness. Their role is critical in ensuring emerging risks are monitored effectively and contingency plans are developed for significant emerging threats, as they are identified. They also need to ensure the organisation has the demonstrated capability to respond to a range of strategic, operational, financial, and environmental threats.

By ensuring an adequate level of preparedness has occurred and that capability exists at all levels to respond effectively to crisis events, organisations can respond quickly, resume business operations and minimise losses.

RESOURCES

To access more resources, visit the links below.

Cyber Resilience: What does good look like?
www.janellis.com.au/cyber-resilience-what-does-good-look-like

Cyber Resilience Scorecard
www.janellis.com.au/cyber-resilience-scorecard

Cyber Resilience

Cyber Resilience Scorecard

Cyber Crisis Response Overview

Cyber Resilience Professional Accreditation Program

Cyber Resilience Accreditation Program 1-pager

Cyber Response Resources

Scenario Planning

Executive Level Digital War Room

Janellis Decision Support Tool

Organisational Resilience

What is Organisational Resilience?

Qantas Organisational Resilience Case Study

Janellis Organisational Resilience Framework

Organisational Resilience Framework Technical Version

Convergence: The National Emergency Summit, Sydney 2006

Organisational Resilience Expertise

Critical Thinking

Critical Thinking Framework

Critical Thinking Professional Accreditation Program

Critical Thinking Accreditation 2-pager

Guide to Exceptional Thinking–White Paper

Embedding High-Quality Decision-Making across the Enterprise Roadmap

Cyber Resilience Case Studies

Australian Superannuation company

Leading Australian Government Agency

Leading Organisation in the Aviation Industry

APPENDIX 1

ORGANISATIONAL RESILIENCE FRAMEWORK—TECHNICAL

1

Protect the organisation through the identification & mitigation of critical risks

1.1
Enterprise View of all Risks
An integrated approach to managing all strategic operational and financial risks.

1.2
Catastrophic Risk Management
Identification, monitoring and reporting of catastrophic risks.

1.3
Emerging Threats
Contingency plans for a range of potential emerging threats.

1.4
Critical Dependencies
Documentation of the risks and vulnerabilities of critical suppliers and other third parties.

1.5
Scenario-based Modelling
Scenario based modelling to consider a range of possible futures and inform decisions.

2

Minimise impact to people and business through preparation and planning

2.1
Readiness Strategy
An overarching approach to creating resilience across the organisation.

2.2
Stakeholder Management
Stakeholder management plan with pre-considered strategies to manage communications.

2.3
Plans & Procedures
Plans and procedures that reflect the current risk profile of the organisation.

2.4
Equipment, Facilities & Tools
Contingency planning and testing of equipment, facilities and tools against a range of scenarios.

2.5
Training & Awareness
Training and awareness to develop the knowledge and skills of individuals and teams.

3

Optimise team performance for BAU and crisis events

3.1
Response Strategy
Response strategy to build the capability using desktop scenarios, hypotheticals or exercises.

3.2
Exercise Development
Robust and integrated scenario-based activities using current and emerging threats.

3.3
Communications
Stakeholder matrix with pre-considered communications messages and time expectations.

3.4
CM Leadership & Critical Thinking
Exercising and testing to focus on dealing with an escalating and/or uncontrolled situation.

3.5
Learning & Development
Clear Post Incident Review (PIR) and follow up methodology.

4

Governance and reporting of resilience capability to provide assurance

4.1
Governance Structure
A formal governance process to ensure a consistent application of the overarching policy.

4.2
Reporting
Integrated reporting on all strategic, operational and financial risks and threats.

4.3
Surveys
Surveys follow major events and simulations to gauge confidence and feedback.

4.4
Benchmarking
Benchmarking to highlight key areas of competency or vulnerabilities.

4.5
Audits
Internal audits: self-assessments, observations and compliance checks.

References

[1] Australian Financial Review. 2023. Seven steps to dealing with the COVID-19 crisis. [ONLINE] Available at: https://www.afr.com/work-and-careers/leaders/seven-steps-to-dealing-with-the-covid-19-crisis-20200325-p54dvy. [Accessed 23 November 2023].

[2] CISCO Systems. 2023. Cisco Cyber Security Readiness Index March 2023. [ONLINE] Available at: https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf. [Accessed 14 April 2023].

[3] IBM. 2023. Cost of a Data Breach Report 2022. [ONLINE] Available at: https://www.ibm.com. [Accessed 14 April 2023].

[4] Cybercrime Magazine. 2021. Cybersecurity Market Report. [ONLINE] Available at: https://cybersecurityventures.com/. [Accessed 28 October 2022].

[5] Australian Government – Australian Cyber Security Centre. 2022. Preparing for and Responding to Cyber-Security Incidents. [ONLINE] Available at: https://www.cyber.gov.au/acsc/view-all-content/publications/preparing-and-responding-cyber-security-incidents [Accessed 27 October 2022].

[6] MIT Sloan Management Review. 2023. An Action Plan for Cyber Resilience. [ONLINE] Available at: https://sloanreview.mit.edu/article/an-action-plan-for-cyber-resilience/. [Accessed 14 April 2023].

[7] Australian Financial Review. 2022. Medibank, Optus hacks: 'Human stupidity' the likely cause, says top cybersecurity expert. [ONLINE] Available at: https://www.afr.com/technology/human-stupidity-likely-cause-of-medibank-optus-breaches-20221025-p5bsqu. [Accessed 27 October 2022].

[8] Australian Financial Review. 2023. GPT-4: How ChatGPT is helping cybercriminals attack your business". [ONLINE] Available at: https://www.afr.com/technology/forget-clunky-language-clues-chatgpt-becomes-hackers-new-weapon-20230317-p5ct5f. [Accessed 14 April 2023].

[9] Australian Financial Review. 2023. Microsoft says a downturn could make surging cyberattacks worse. [ONLINE] Available at: https://www.afr.com/chanticleer/microsoft-says-a-downturn-could-make-cyber-threat-worse-20230218-p5clld. [Accessed 18 April 2023].

[10] IBM. 2022. Cost of a Data Breach Report 2022. [ONLINE] Available at: ibm.com.au [Accessed 6 March 2023]

[11] CISCO Systems. 2023. Cisco Cyber Security Readiness Index March 2023. [ONLINE] Available at: https://www.cisco.com/c/dam/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index/2023/cybersecurity-readiness-index-report.pdf. [Accessed 14 April 2023].

[12] Australia launches cyberattack 'war games' for major banks. 2023. Australia launches cyberattack 'war games' for major banks. [ONLINE] Available at: https://amp.smh.com.au/politics/federal/consider-what-damage-could-be-caused-government-launches-cyber-war-games-for-major-banks-20230410-p5czbj.html. [Accessed 14 April 2023].

[13] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023. [ONLINE] Available at www.thebci.org [Accessed on 7 March 2023].

[14] Australian Institute of Company Directors. 2023. Cyber Security Governance Principles. [ONLINE] Available at: https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-governance-principles-web3.pdf. [Accessed 23 November 2023].

[15] Australian Institute of Company Directors. 2023. Cyber Security Governance Principles.

[16] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023. [ONLINE] Available at www.thebci.org [Accessed on 7 March 2023].

[17] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023.

[18] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023.

[19] Lehr, Thomas; Lorenz, Ullrich; Willert, Markus; Rohrbeck, René (2017). "Scenario-based strategizing: Advancing the applicability in strategists' teams". Technological Forecasting and Social Change. 124: 214–24.

[20] Ringland, Gill (2010). "The role of scenarios in strategic foresight". Technological Forecasting and Social Change. 77 (9): 1493–1498.

[21] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023.

[22] IBM. 2022. Cost of a Data Breach Report 2022. [ONLINE] Available at: ibm.com.au [Accessed 6 March 2023]

[23] Ringland, Gill (2010). "The role of scenarios in strategic foresight". Technological Forecasting and Social Change. 77 (9): 1493–1498.

[24] Australia launches cyberattack 'war games' for major banks. 2023. Australia launches cyberattack 'war games' for major banks. [ONLINE] Available at: https://amp.smh.com.au/politics/federal/consider-what-damage-could-be-caused-government-launches-cyber-war-games-for-major-banks-20230410-p5czbj.html. [Accessed 14 April 2023].

[25] Australian Financial Review. 2023. Cyberattacks: Coles' Steven Cain wants regulatory framework for companies. [ONLINE] Available at: https://www.afr.com/companies/retail/coles-boss-puts-onus-on-government-for-clearer-cybersecurity-rules-20221027-p5btmh. [Accessed 14 April 2023].

[26] The Business Continuity Institute, 2023. BCI Cyber Resilience Report 2023. [ONLINE] Available at www.thebci.org [Accessed on 7 March 2023].

[27] World Economic Forum. 2023. Global Cybersecurity Outlook Report. [ONLINE] Available at: https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf. [Accessed 14 April 2023].

[28] World Economic Forum. 2023. Global Cybersecurity Outlook Report.

For more information **W: www.janellis.com.au** | **E: info@janellis.com.au** | **P: +61 2 9994 8914**

About Janellis

Janellis is an enterprise management consulting firm, helping organisations execute strategy and build resilience. We have niche expertise in working with executive leaders to navigate their most complex challenges, threats, and opportunities.

Our Organisational Resilience Framework has been embedded within organisations in industries as diverse as aviation, banking and finance, construction, education, emergency services, government, insurance, hydro, manufacturing, power, technology, transport, telecommunications, and utilities.

Teams use our Critical Thinking Framework to enable agile and robust team-based decision-making. The framework helps cross-functional teams find 'common ground' when looking at both risk and opportunity. It is used at all levels of the organisation including executive leadership teams, risk teams and other teams responsible for complex decision-making.

To learn more, visit: www.janellis.com.au

Clients

The organisational resilience frameworks and tools recommended in this paper have been used to uplift resilience capability for organisations including:

AirServices Australia; AMP; AON; AstraZeneca; Brisbane Airport; BT Financial Group; Commonwealth Bank; Dexus; Property Group; Qantas; Queensland Rail; Hunter Water; iCare; Jemena; John Holland; Leighton Holdings; Lendlease; NSW Roads & Maritime Services; NSW State Emergency Service; NSW Health; QBE; Snowy Hydro; Stockland; Sydney Water; TfNSW; Transfield Services; Virgin Australia; Vodafone; and Westpac Banking Corporation.

Janellis