

Beyond IT Security: The Evolving Obligations of Australian Organisations for Cyber Resiliency

Report Author

Claus Mortensen

Principal Analyst, Ecosystem



Introduction

The surge in digital business transformation over the last few years has propelled the adoption of cloud services, mobile applications, and remote data access. There has also been a significant increase in the use of web and mobile applications for employees and customers alike. Large volumes of data are now being made available across potentially vulnerable attack surfaces and at the same time, cyber adversaries are getting increasingly sophisticated as they start using AI tools to attack organisations worldwide.



58% of technology leaders in Australia feel that a data breach is inevitable within the next year.

Ecosystem Cyber Security Study, 2024

The threat landscape has materially changed, requiring new approaches to cyber security that help organisations detect threats early, reduce the impact of an attack, and minimise risk and damage to the business.

Cyber security has become a key topic of discussion at the board level, raising equal concerns among business and technology leaders. CEOs and business leaders now require a comprehensive understanding of the compliance landscape and the ramifications of incidents and breaches, while technology leaders tasked with implementing transformative technologies must grasp their impact on the threat landscape. Meanwhile, cyber leaders face the challenge of adopting effective technologies to proactively combat threats. A comprehensive cyber strategy should consider the impact on people management, compliance and risk practices, as well as technology investments.

This whitepaper explores the implications of Australia's evolving cyber security landscape for key stakeholders, including boards, company directors, business leaders, and technology leaders.



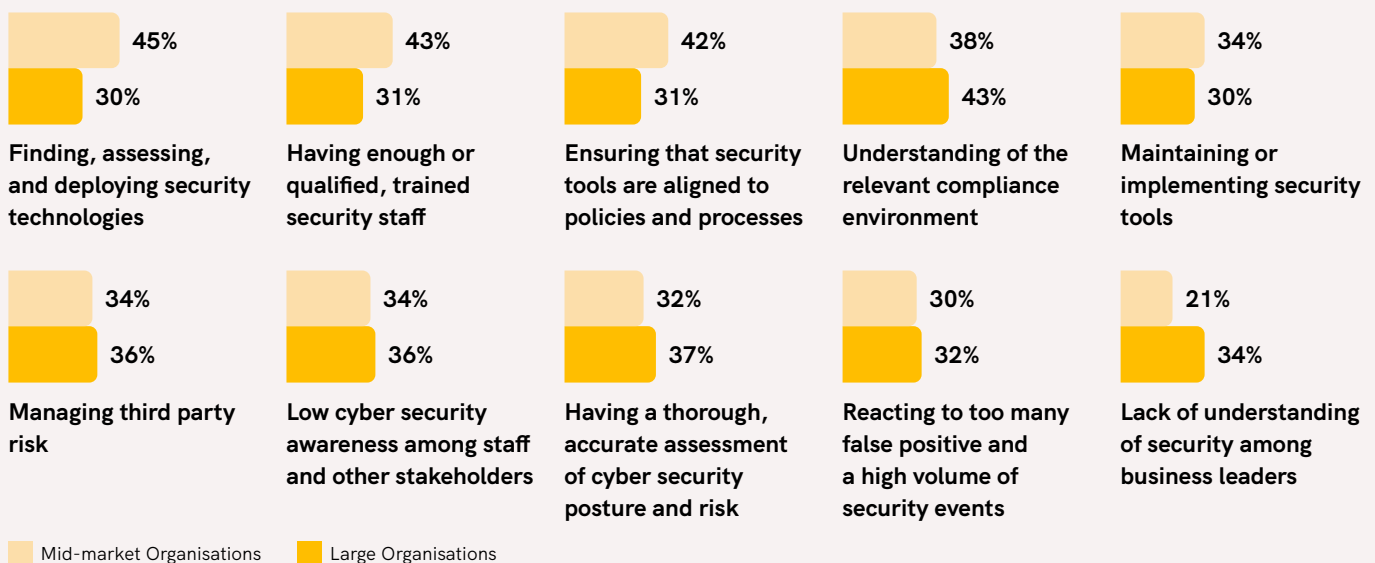
Current Threats and Future Trends

In recent years, organisations have had to find new ways to engage and connect with customers and employees. Cyber security was not always the main consideration as organisations scrambled to cope with rapidly changing market demands. The resulting increase in attack surfaces continues to grow – especially as employees access company networks and data from multiple locations and devices.

The primary cyber challenges faced by organisations vary greatly based on their size. Large organisations are often preoccupied with compliance and risk management, while smaller entities tend to struggle more with technological and people-related issues (Figure 1).

While challenges might be different, what is universal is that crafting a robust cyber security strategy requires a comprehensive plan. This plan should outline the organisation's approach to identifying, managing, and mitigating cyber security risks.

Figure 1: Cyber Challenges in Australia Differ Based on Organisational Size



N=204 (Australia)

Source: Ecosystem Cyber Security Study, 2024

Note: Mid-market organisations employ 101-500 employees



While many organisations claim to have a cyber security strategy, they often limit themselves to compartmentalised tactical plans addressing specific breach scenarios rather than a holistic strategy spanning the entire organisation.

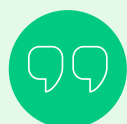
A robust cyber strategy requires an understanding and involvement in four key areas

- Compliance Management
- People and Stakeholder Involvement
- Incident Response Planning
- Risk-Based Vulnerability Management

#1 Compliance Management

Cyber security regulations and compliance requirements play a vital role in protecting sensitive data and managing cyber risks. In Australia, these regulations evolve continually, often in response to high-profile breaches. Adhering to specific laws is crucial for organisations to maintain the integrity and security of their digital assets. With an anticipated increase in regulatory scrutiny due to continued cyber security breaches, organisations should as a minimum follow both general and industry-specific guidelines.

The Australian Privacy Principles (APP) provide the guidance on Australia's cyber compliance and require organisations to take reasonable steps to protect information from misuse, interference, loss, unauthorised access, modification, or disclosure. Additionally, under the Notifiable Data Breaches (NDB) scheme, any organisation covered by the Privacy Act must inform affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is expected to cause serious harm to an individual whose personal information is involved. To complicate the compliance landscape, additional sector-specific regulations apply – particularly within financial services, critical infrastructure, the public sector, and health services. Although not all are mandatory, they are commonly seen as best practices.



When evaluating cyber security measures, it is crucial to distinguish between frameworks and standards. A framework provides the overall structural support for a system, offering flexibility for organisations to tailor it to their needs. Standards, however, are structured sets of procedures and controls recognised by certification bodies, often globally acknowledged like ISO. Standards provide an industry-aligned level of protection, frequently needed for collaborations with government, healthcare, banks, and other entities requiring an added level of information security.

Key Steps to Compliance Management

- 1. Understand and adhere to Australian regulatory requirements**

Privacy Act	ACSC	ISO/ISMS
NDB	ASD	Industry-specific regulations and standards
- 2. Develop a robust risk management framework**
- 3. Establish clear cyber security policies and procedures**
- 4. Perform a gap analysis on the alignment of cyber policies and measures**
- 5. Implement strong access controls and data protection measures**
- 6. Formulate an incident response plan involving all stakeholders**
- 7. Conduct training and awareness sessions for all employees**
- 8. Assess and audit compliance regularly with a focus on continuous improvement**

The Essential 8 Framework and its significance in bolstering security posture

Compliance management involves a series of steps and considerations to ensure an organisation's adherence to laws, regulations, standards, and best practices. In Australia, organisations often follow the Essential 8 cyber security guidelines, established by the Australian Cyber Security Centre (ACSC), which outline fundamental measures to enhance cyber resilience.

The Essential 8 is a prescriptive minimum baseline for cyber security. They are just that – essential. They consist of the most important 37 prioritised strategies for organisations to mitigate cyber incidents, developed by the ACSC in 2017. The most recent changes to the guidelines were introduced in [November 2023](#). Broadly speaking, the Essential 8 has three strategy categories.



Strategies to prevent attacks:

- Application control and whitelisting
- Application patching
- Microsoft Office macro management
- Multi-factor authentication



Strategies to compartmentalise or limit attacks:

- User application hardening
- Restricting administrative privileges
- Patching operating systems



Strategies to recover from attacks:

- Regular backups

It is a good resource for organisations that want a simple checklist approach to cyber security.

It is however important to understand what the Essential 8 does not do.

- It does not provide a framework for more integrated approaches to organisational cyber security. This suggests that the Essential 8 may not offer sufficient coverage for the cyber security requirements of larger organisations.
- It does not account for business activities and behavioural elements that might contribute towards risks. This means that the Essential 8 is not suited for the broader approach to risk-based vulnerability management.

Other major frameworks and standards that Australian leaders should be aware of include:

● **The Australian Prudential Regulation Authority (APRA)** introduced CPS 234, requiring robust IT security measures within the **financial** and **insurance** sectors. According to this prudential standard, regulated entities should implement IT security practices adequate to the threat that they face. Key requirements include information asset classification, security control implementation, incident management protocols, testing, and auditing. Clear delineation of roles and responsibilities for the board, senior management, and governing bodies is essential to ensure accountability. In the event of a breach, organisations must promptly respond and notify APRA without delay.

● **Protective Security Policy Framework (PSPF)** is critical for Australian **government** entities and non-corporate Commonwealth entities, and is considered a best practice for Australian states. The framework aims to help entities protect their information, personnel, and assets.

● **Australian Energy Sector Cyber Security Framework (AESCSF)** blends recognised security frameworks with a risk-management approach and is recommended for the Australian **energy** sector. AESCSF is both a framework and an annual voluntary assessment program.

● **The Security of Critical Infrastructure Act 2018 (SOCI Act)**, strengthened by amendments from the Security Legislation Amendment Critical Infrastructure Protection Act 2022 (SLACIP), aims to safeguard **critical infrastructures** from foreign cyber threats. SLACIP extends the scope of SOCI to encompass 11 sectors, including energy, education, data storage, financial services, health and medical services, grocery and food, space technology, and transport.

The SLACIP Act introduces two key elements: The Critical Infrastructure Risk Management Program (**CIRMP**), mandating sectors to identify and mitigate various hazards, and the Enhanced Cyber Security Obligations for Systems of National Significance (**SoNS**). SoNS assets, vital for Australia's society, economy, and security, must comply with enhanced cyber security measures, including the development of Cyber Security Incident Response Plans.

● **Information Security Manual (ISM)** from the Australian Signals Directorate outlines cyber security principles for governance, protection, detection, and response. The manual also provides CIOs and CISOs with practical guidelines that can be applied using a **risk-based** approach to security.

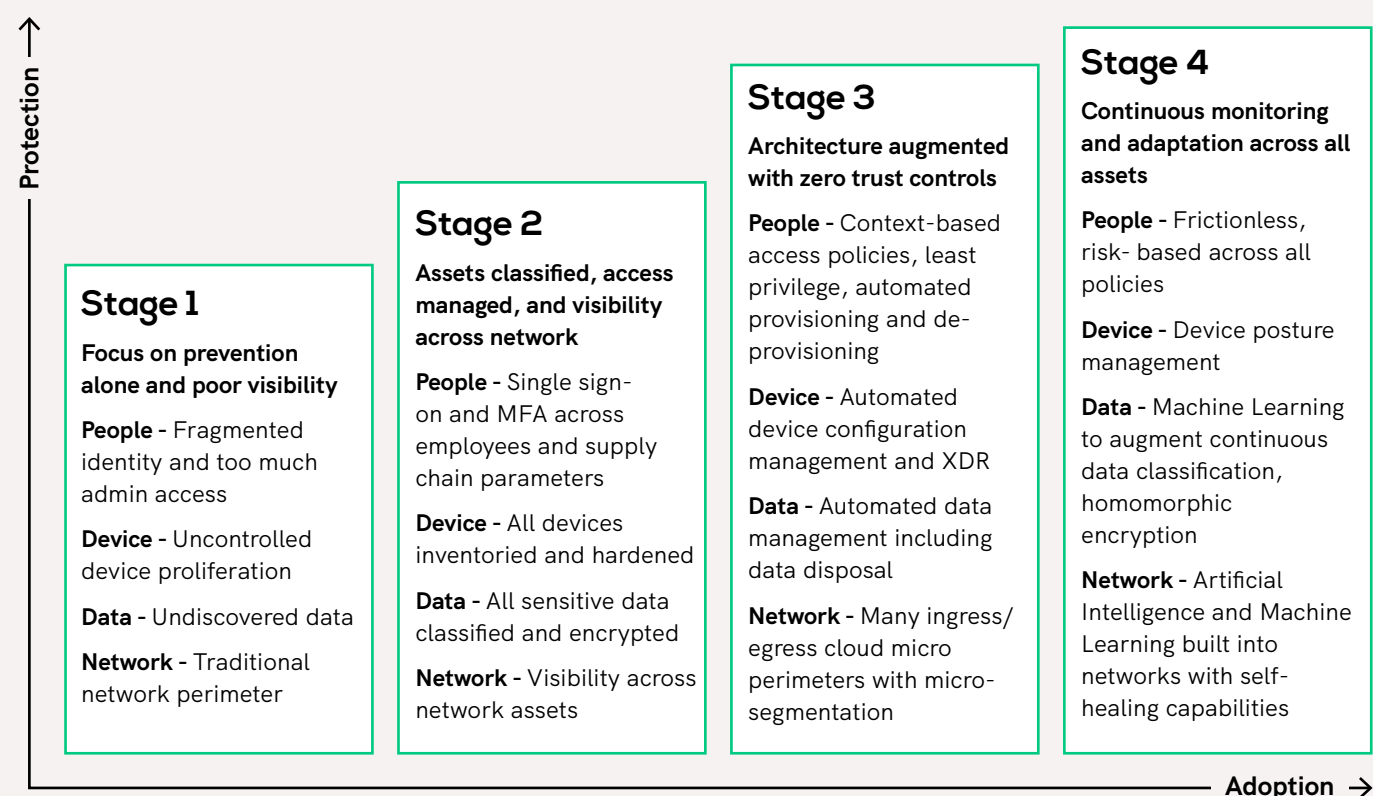
● **ISO 27001** is the **international** standard for information security and is essential for showcasing the strength of the security posture to prospects and customers worldwide. It provides the framework and guidelines for establishing, implementing, and managing an information security management system (ISMS), and offers best practices for managing information security through people, processes, and technology.

● **Other Standards and Frameworks:** Include SOC 2, NIST Cyber Security Framework (CSF), Control Objectives for Information Technology (COBIT), Cloud Control Matrix (CCM), and CIS Critical Security Controls. PCI DSS is the standard for any organisation processing payment cards. Many Australian organisations operating internationally may also find that they are affected by foreign legislations – the EU's General Data Protection Regulation (GDPR) being a prime example.

Compliance and Maturity

Navigating the Australian compliance landscape can be confusing, especially when organisations need to adhere to multiple frameworks and standards. Despite compliance efforts, many technology and business leaders may remain uncertain about the maturity of their cyber strategies and practices. As business leaders increasingly become key stakeholders in an organisation's cyber strategy, Ecosystm has developed a model that provides a high-level view of organisations' cyber maturity by breaking cyber security controls into four categories – People, Devices, Data and Networks (Figure 2).

Figure 2: The Cyber Maturity Journey



Source: Ecosystm, 2024

Ecosystm research shows that many Australian companies either fail to classify their data or have not embraced critical access controls. This would place most Australian organisations between stages 1 and 2.



Living up to mandatory security requirements may be enough to escape liability or legal penalties in case of a breach, but it is not necessarily enough to avoid breaches from happening at all. All organisations should understand that while being compliant is a good indicator for how well an organisation is prepared to cope with cyberattacks, rules and standards should be seen as minimum requirements – not as a ceiling. Being compliant does not in itself mean organisations are safe. Organisations should continuously evaluate their existing solutions considering the changing threat landscape. Mature organisations view each security audit as an opportunity to improve their security posture and enable new levels of transformation. Engaging an external partner is often the best approach to bring different and more open perspectives to the table.

#2 People and Stakeholder Involvement

Organisations face significant challenges concerning their people. This includes the need for an executive team that prioritises robust cyber strategies; finding and retaining the right cyber talent to navigate the diverse and evolving threat landscape; and driving awareness on cyber threats, measures, and responsibilities among all employees.

Executive Accountability



75% of technology leaders in Australia feel that senior leadership has an inadequate understanding of cyber risk and governance.

Ecosystem Cyber Security Study, 2024

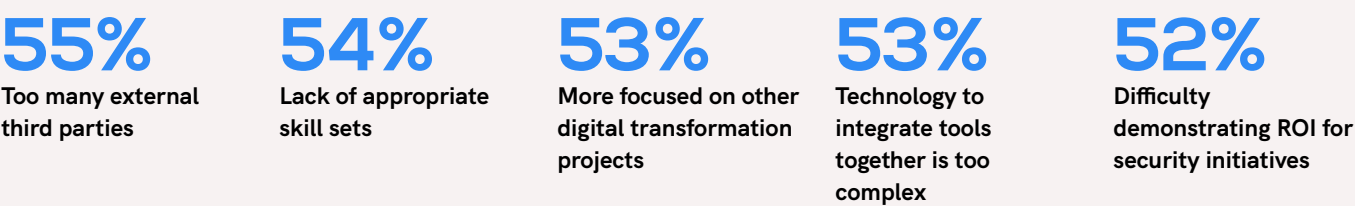
Senior leadership and the board have a pivotal role in the oversight of cyber strategies, risk management, and reporting obligations. As stewards of corporate governance, they are responsible for setting the tone for the organisation's cyber culture and ensuring that cyber security is integrated into overall business strategies. Senior leadership has the primary responsibility of establishing robust risk management frameworks, allocating resources for cyber initiatives, and promoting a culture of accountability and awareness throughout the organisation. The board should provide oversight and guidance on cyber risk management, regularly assessing the effectiveness of cyber security measures, and ensuring compliance with regulatory requirements. They have a larger role to play as well, in ensuring that cyber risks are effectively communicated to stakeholders and that appropriate reporting mechanisms are in place to address any potential threats or breaches promptly. Ultimately, the active involvement of senior leadership and the board is essential in safeguarding the organisation against cyber threats and maintaining stakeholder trust and confidence.

Skills Shortage

The scarcity of skills is particularly acute in cyber security compared to other technology areas. Recruiting talent has become costly due to the skills shortage and resulting competition. The increasing workload on security operations has also made retaining talent challenging, with employees often experiencing burnout quickly. However, safeguarding multiple systems and cloud applications against vulnerabilities is imperative and requires additional specialists such as security analysts, engineers, threat researchers, and incident response managers. Many organisations simply lack the resources to attract and retain cyber security talent.

Organisations find that outsourcing to MSSPs offers the scalability and access to automated tools needed for round-the-clock vigilant monitoring, effectively addressing the challenges posed by the cyber security skills shortage. Ecosystem research highlights the lack of skills as a major challenge to organisations with more than half saying that they lack the appropriate skills when it comes to managing application security initiatives, in particular (Figure 3). This is compounded by the number of third-party cyber tools that internal staff must navigate to gain visibility.

Figure 3: Top 5 Challenges of Managing Application Security in Australia Highlight Skills Shortage



Q: What are your organisation's top 5 challenges in managing application security initiatives?
N=204 (Australia)
Source: Ecosystem Cyber Security Study, 2024

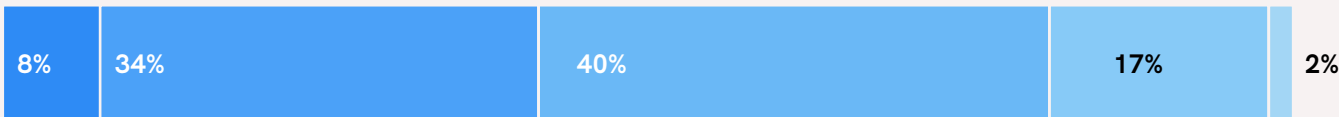
Alert Fatigue

Security operations teams must contend with the thousands of alerts that they receive each day. As a result, security analysts suffer from alert fatigue and struggle to recognise critical issues and novel threats. Monitoring tools have improved network visibility but also contribute to increased volumes of data that security operation centres (SOCs) must parse. There is an urgency to deploy solutions that can help to reduce noise. For many organisations, an AI-augmented security team could deprioritise 90% of alerts and focus on genuine risks. This can be done by correlating alerts to help analysts see patterns in the data and identify root causes faster. Systems that prioritise alerts also allow SOCs to attend to the most critical events first.

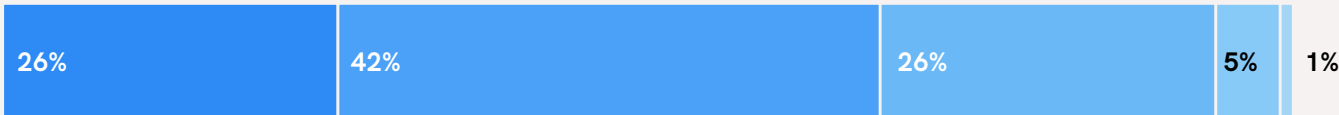
Although many Australian organisations are addressing this issue by increasingly relying on automation, many others falter, especially smaller organisations. While 68% of large organisations rely on automation, only 42% of mid-market organisations do so even though their cyber security concerns are mainly identical (Figure 4).

Figure 4: Mid-Market Organisations in Australia Lagging in Cyber Automation

Mid-market Organisations



Large Organisations



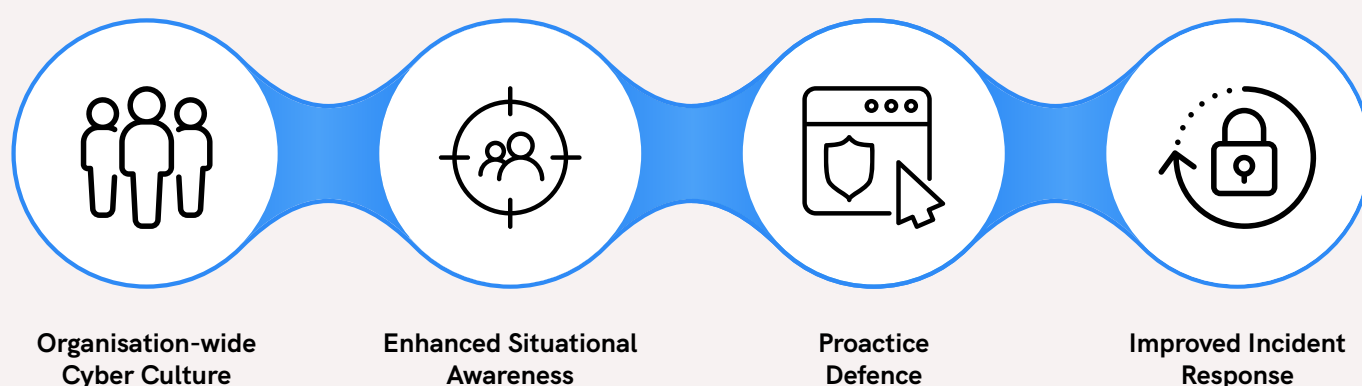
5 (Very High) 4 3 2 1 (Low)

Q: Rate the extent of automation of cyber security processes in your organisation (on a scale of 1-5).
Source: Ecosystem Cyber Security Study, 2024
Note: Mid-market organisations employ 101-500 employees

Threat Intelligence

Emerging ransomware, phishing, and cloud vulnerabilities exploit the expanding digital attack surface of organisations. Security operations teams are overwhelmed with alerts, leaving little time for proactive threat investigation. To augment internal threat hunting efforts, organisations need a partner with a scalable security data lake. Threat intelligence providers aggregate insights from diverse client engagements and dedicated researchers. Dark web research enhances situational awareness, offering predictive capabilities beyond what individual organisations can achieve. Regular reporting keeps CEOs, business leaders, and technology leaders informed of evolving threats, reassuring them of their organisations' cyber practices.

Key Steps to People and Stakeholder Empowerment



While cyber skills are difficult to find and retain, that is not the only people-related issue that organisations face. One of the key challenges for organisations is the lack of awareness of cyber risks and protocols across all employees. Organisations have become better at prioritising training and awareness programs, educating employees about common threats like phishing and best practices for safeguarding sensitive data. While these programs are often ongoing and adaptable to new threats, they can sometimes become mere compliance checklists, raising questions about their true effectiveness. Conducting simulated phishing attacks and security quizzes to assess employee awareness and identifying areas where further training is required, can be effective.

To truly educate employees on risks, it's essential to move beyond compliance and build a cyber security culture throughout the organisation. This can involve setting organisation-wide security KPIs that cascade from the CEO down to every employee, promoting accountability and transparency. Creating an environment where employees feel comfortable reporting security concerns is critical for early threat detection and mitigation.

#3 Incident Response Planning



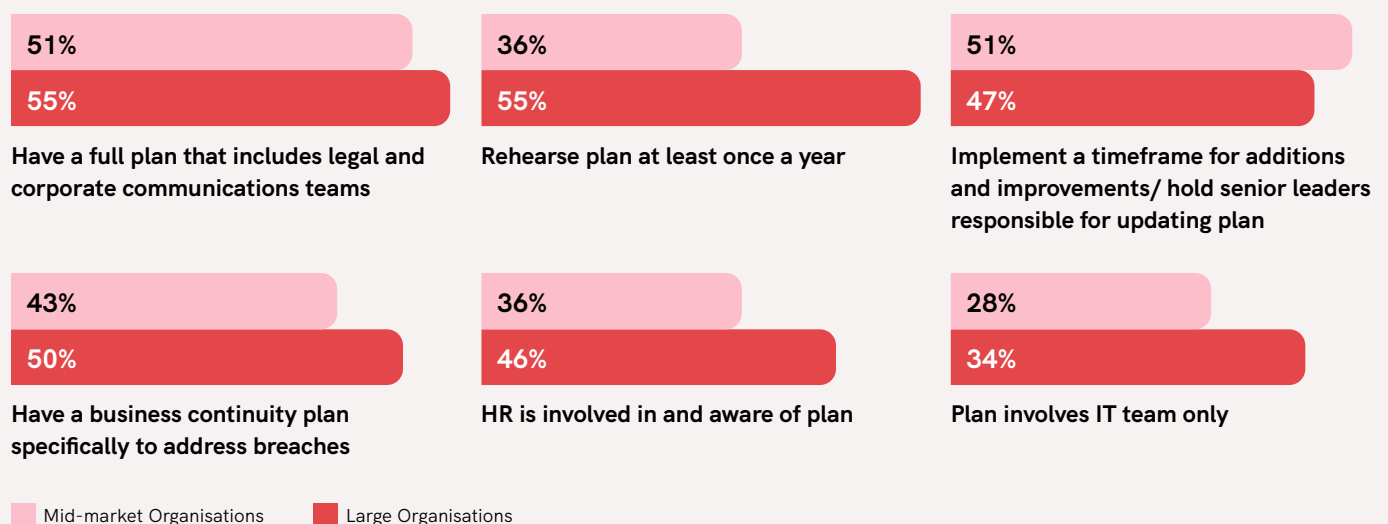
27% of Australian organisations state that inadequate incident response plans are a major cyber security concern.

Ecosystem Cyber Security Study, 2024

Clear security policies and enforcement are essential to ensure employees understand their roles within the broader security framework, including responsibilities on strong password use, secure data handling, and prompt incident reporting. However, despite the best efforts, breaches do happen – and this is where a well-defined incident response plan is crucial to minimise the damage. This requires every employee to know their roles and responsibilities during a security incident.

Analysing why many Australian organisations think that their incident response plan is inadequate, we find that just over half of Australian organisations have a comprehensive plan that involves legal and corporate communications teams – aimed at mitigating both legal and reputational risks (Figure 5). Almost a third of organisations say their plans only involve the IT team. Mid-market organisations in particular are less likely to re-evaluate their incident response plan to address newer threats that appear on the horizon.

Figure 5: Mid-Market Organisations in Australia Lagging in Cyber Automation



N=204 (Australia)

Source: Ecosystem Cyber Security Study, 2024

Note: Mid-market organisations employ 101-500 employees

The importance of a comprehensive and robust incident response plan to the continuity and even survival of a business in case of major cyber security breaches cannot be overstated – especially since almost 60% of organisations believe such incidents are inevitable.

Many organisations do not have comprehensive plans either due to a lack of skills or bandwidth. Additionally, one-third of organisations indicate a challenge in ensuring alignment between their tools and policies and processes. Therefore, even those with incident response plans in place may lack the tools needed to effectively execute these plans.

Key Considerations of a Robust Incident Response Plan

- **Business Continuity and Disaster Recovery.** Establish backup systems for data and system restoration during incidents. Plan for worst-case scenarios where critical operations or data may not be recoverable promptly or multiple systems are impacted simultaneously.
- **Stakeholder Management.** Identify stakeholders, such as employees, regulators, customers, shareholders, the media and so on. Assign responsibilities for engaging with stakeholders. Develop key messages and holding statements for various cyber-attack scenarios.
- **Breach Response.** Ensure understanding of personal and sensitive data held and its locations. Develop a comprehensive plan outlining when to notify individuals and provide support and advice to mitigate financial and non-financial risks.
- **Regulator Response.** Identify regulatory reporting obligations and timeframes. Ensure adequate resources and expertise to anticipate and respond to regulators' inquiries and investigations. Establish procedures for obtaining additional resources if needed.
- **Decision Guidance.** Develop operational and technical plans for foreseeable cyber incidents, such as system outages, ransomware attacks, DDOS attacks, data theft, third-party compromise, and credential compromise attacks.
- **Training and Simulation.** Establish a comprehensive training program, including whole-organisation and team-based simulations. Conduct training for diverse scenarios aligned with risks and emerging threats. Update plans and training based on lessons learned.
- **Third-party Provider Management.** Identify contacts for incident response. Ensure IT providers have adequate resources for support. Conduct due diligence on providers as per insurance panel arrangements. Identify resources for legal advice, crisis communications, IT forensics, ransom negotiation, and crisis management support.



Incident response plans are crucial and sometimes mandatory, driven by compliance requirements. Organisations should conduct regular incident response simulations to help employees gain experience and build confidence under pressure. Additionally, unforeseen gaps in the plan can be identified during post-exercise assessments.

Organisations that have doubts about their current response plans or capabilities should consider seeking external help. Even organisations that believe that their response plans are comprehensive and robust, should put it to the test by a trusted external partner – as part of an evaluation of the overall security strategy.

#4 Risk-Based Vulnerability Management

The annual count of tracked vulnerabilities continues to reach new highs, presenting a daunting challenge for cyber leaders. This requires conducting vulnerability assessments to identify pertinent issues and devising strategies for mitigation. The task becomes more complex with the proliferation of distributed and heterogeneous systems.

Technology and cyber leaders acknowledge the significant risk posed by exploited vulnerabilities within their organisations. While nearly all organisations have tools for vulnerability assessment, a robust vulnerability management system considers the risks that the organisation faces.

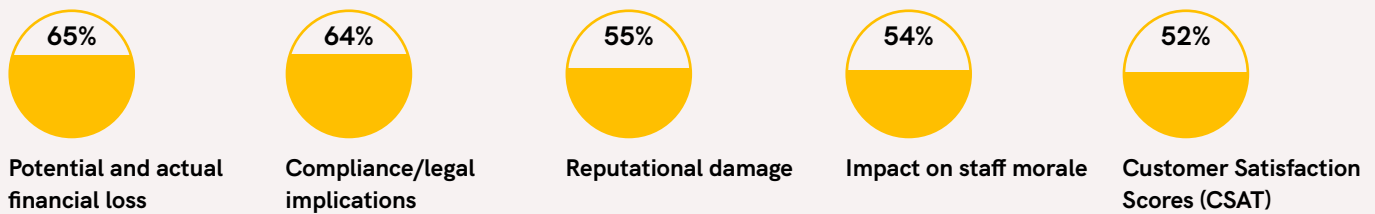
Understanding Risk

Vulnerability management requires a comprehensive understanding of cyber security breaches and their impact across the organisation. Traditional methods treating all vulnerabilities equally are impractical and organisations need a more nuanced strategy. These risks include:

- 1 Business Continuity**
System downtime or ransomware attacks, disrupting core functions and potentially forcing business shutdowns
- 2 Competitive Risk**
Exposure of sensitive corporate data, such as strategic plans or proprietary information, to malicious actors
- 3 Customer Risk**
Compromise of sensitive customer data, leading to privacy concerns and potential legal implications
- 4 Reputational Risk**
Potential damage to image, impacting customer trust and regulatory relationships
- 5 Regulatory Risk**
Regulatory scrutiny and reporting under frameworks like the APPs or the APRA prudential standards
- 6 Legal Costs**
Legal expenses, including fees for lawyers, fines, and liabilities resulting from legal action
- 7 Societal Risk**
Broader societal implications, as outlined by regulations such as the SOCI Act and the SLACIP

A better and more holistic understanding of how cyber security breaches affect the organisation allows for a new, risk-based approach to how vulnerabilities can be managed. This is still a challenge for many organisations. While most organisations include financial loss and compliance implications in their risk assessments, significantly fewer include areas such as reputational damage, impact on employee morale, or customer satisfaction (Figure 6).

Figure 6: Factors Considered for Business Impact Assessment by Australian Organisations



Q: What do business impact assessments to understand the impact of a security incident include in your organisation?

N=204 (Australia)

Source: Ecosystem Cyber Security Study, 2024

Integrating a risk-based approach with automation in vulnerability management allows organisations to effectively identify, prioritise, and mitigate security vulnerabilities based on their impact on the organisation.

A risk-based approach, combined with AI, automation, and security information and event management (SIEM) platforms can significantly enhance cyber security effectiveness. However, implementing these measures can be complex and resource-intensive for organisations.

For mid-market organisations in particular, that are often targeted by cybercriminals due to perceived vulnerabilities, vulnerability management platforms (VMPs) are crucial. While VMPs can be implemented on-premises, this requires initial and ongoing investments in infrastructure and cyber training. Many mid-market organisations may find it more practical to engage a service provider for vulnerability management, benefiting from threat management, automated responses, and enhanced visibility over assets and vulnerabilities through customisable dashboards and reports. A competent service provider can offer guidance and support in conducting comprehensive risk assessments, including those mandated by local authorities and regulatory bodies.



Looking at Vulnerability Through a Risk Lens

Risk-based vulnerability management (RBVM) aims to address this challenge by concentrating on vulnerabilities that present the highest risk to the organisation's information assets. Key steps include:

Identifying Risks

Beyond technical aspects, RBVM requires a deep understanding of business risks involving stakeholders across the organisation.

Assigning Ownership

Clear accountability and risk ownership is assigned to relevant staff or business units for prompt resolution.

Prioritising Risks

Risks are evaluated based on probability and severity, with Risk Scores assigned considering severity, potential impact, and likelihood of exploitation, with Criticality Scores for organisational impact assessment.

Addressing Risks

Swift action is taken including software updates, process changes, and other measures to mitigate breach impact.

Reporting and Monitoring

Continuous monitoring and feedback loops inform risk reassessment and reprioritisation in line with gathered data.










A complete understanding of business risk requires the involvement of stakeholders from across the organisation. Given that many IT teams lack the expertise for this, it's essential to garner support from senior management for risk evaluation. Ensuring that the board has visibility over vulnerabilities and the associated risks is crucial. Without their engagement, it becomes difficult to secure additional cyber security resources.

Applying risk-based rules to vulnerability management can also free up resources within cyber security teams and ensure cost-effective management over time.

Conclusion

As technology integrates into essential business functions, the traditional cyber security approach is no longer adequate. A robust cyber security approach requires a comprehensive understanding of how security breaches may affect the organisation and a fundamental grasp of associated business risks. It requires the involvement of stakeholders across the organisation, not solely the CIO and CISO.

To enhance cyber security management:

-  View regulatory compliance and industry standards as minimum requirements rather than end goals. Compliance may mitigate liability in breaches but does not necessarily prevent them.
-  Assess existing solutions continuously against evolving threats. Engaging an external partner can offer diverse perspectives.
-  Embrace automation to address minor threats, reduce false positives, and enhance visibility. Consider outsourcing SOCs and vulnerability management to free up internal resources.
-  Implement ongoing employee training programs to maintain awareness and knowledge. Move beyond compliance to cultivate a cyber security culture throughout the organisation. This includes setting organisation-wide security KPIs that cascade from the CEO down to every employee, promoting accountability and transparency.
-  Develop comprehensive incident response plans and test them regularly with trusted external partners.
-  Apply risk-based rules to vulnerability management to optimise IT security resources and long-term costs. Ensure the board has visibility over vulnerabilities to secure their support for cyber security resource allocation.
-  Engage stakeholders from across the organisation in risk evaluation, supported by senior management and external partners if necessary.

Most importantly, do not adopt a wait-and-see approach, assuming that your current cyber security framework is good enough until proven otherwise. The risk and the potential costs are simply too high.



About the Author

Claus has more than 17 years of experience in both strategic and tactical guidance for vendors and service providers in the IT and telecommunications space. Having worked as an analyst and a consultant in both Europe and Asia, Claus has supported clients with local, regional and global briefs to position their offerings and grow their businesses in their target markets. These have included Google, Microsoft, IBM, AT&T, Orange and SingTel.

Previously, Claus spent nine years at IDC Asia Pacific, where he climbed the ranks to launch and lead IDC's Emerging Technology practice. In Asia and Europe, Claus is also a renowned speaker and blogger, who continues to evaluate and forecast how disruptive technologies impact the marketplace and how digitization is transforming business models across all industries. Claus is based in Copenhagen, Denmark, which also marks Ecosystm's extension and coverage in the EMEA region.

About Ecosystm

Ecosystm is a Digital Research and Advisory Company with its global headquarters in Singapore. We bring together tech buyers, tech vendors and analysts onto one integrated platform to enable the best decisionmaking in the evolving digital economy. Ecosystm has moved away from the highly inefficient business models of traditional research firms and instead focuses on research democratisation, with an emphasis on accessibility, transparency, and autonomy. Ecosystm's broad portfolio of advisory services is provided by a team of Analysts from a variety of backgrounds that include career analysts, CIOs and business leaders, and domain experts with decades of experience in their field. Visit ecosystm.io

About Nexon Asia Pacific

Nexon Asia Pacific (Nexon) is an award-winning digital consulting and managed services partner for mid-market and government organisations across Australia. We have a uniquely broad suite of solutions to service clients who require end-to-end capabilities coupled with specialist expertise in security, cloud, and digital solutions.

Our end-to-end solutions help clients to solve problems, address frictions, and accelerate growth. Committed to the highest standards of responsiveness, competency, and transparency, Nexon is built on a unique client care model that is fuelled by continuous feedback. With 500+ staff, we employ some of the country's most experienced consultants and empower teams to make decisions that accelerate change for client organisations.

As a certified and accredited local and state government provider, CREST, and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative solutions and service excellence.

We help our clients move from a position of overwhelm to empowerment, looking forward to a more agile and digital future.

nexon.com.au

This whitepaper is sponsored by Nexon Asia Pacific. It is based on the analyst's subject matter expertise in the area of coverage in addition to insights from interactions with technology buyers in multiple industries and technology vendors, industry events, and secondary research.

The data findings mentioned in all Ecosystm reports are drawn from Ecosystm's live and on-going studies on the Ecosystm research platform. For more information about Ecosystm visit ecosystm.io