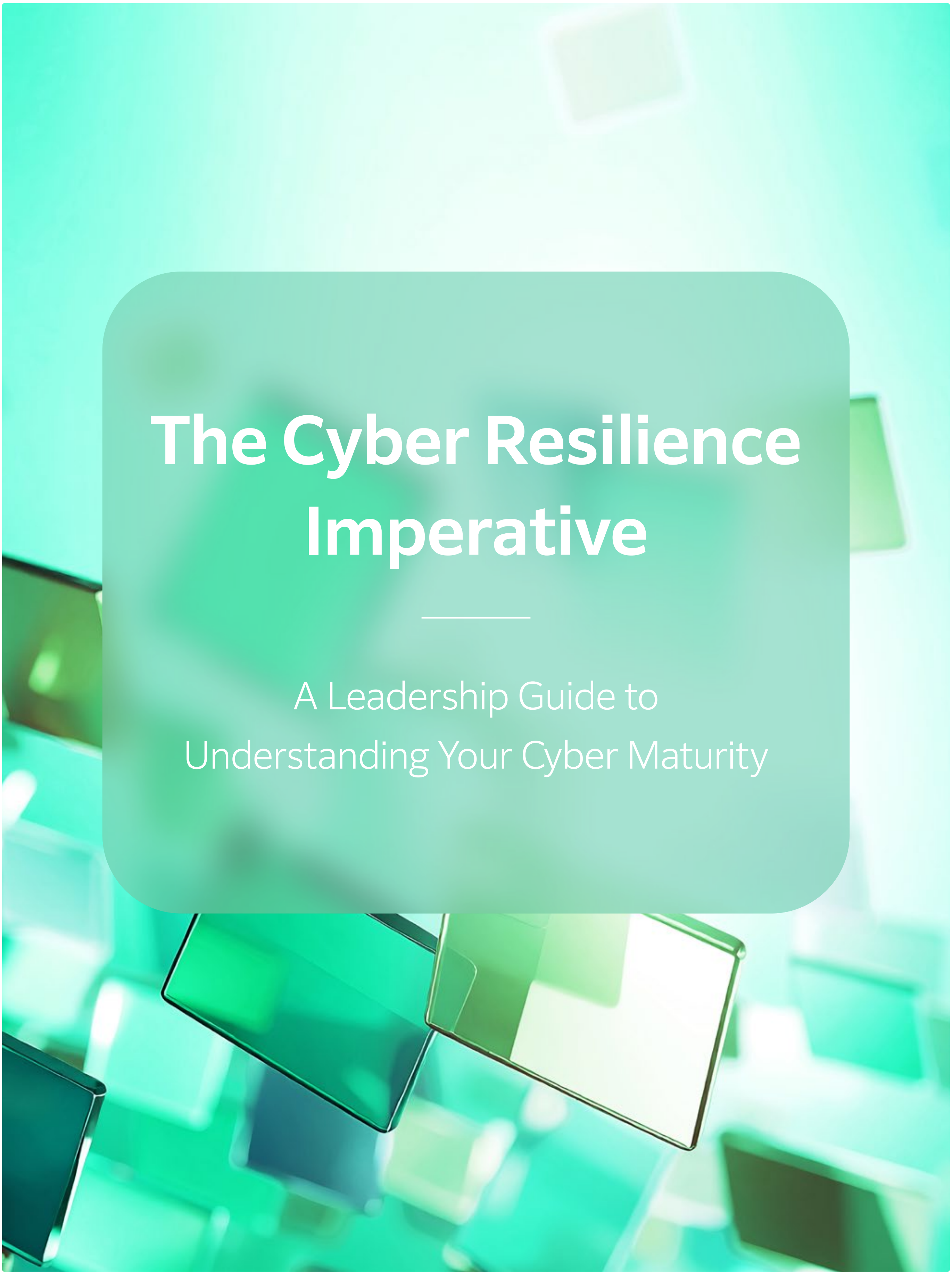
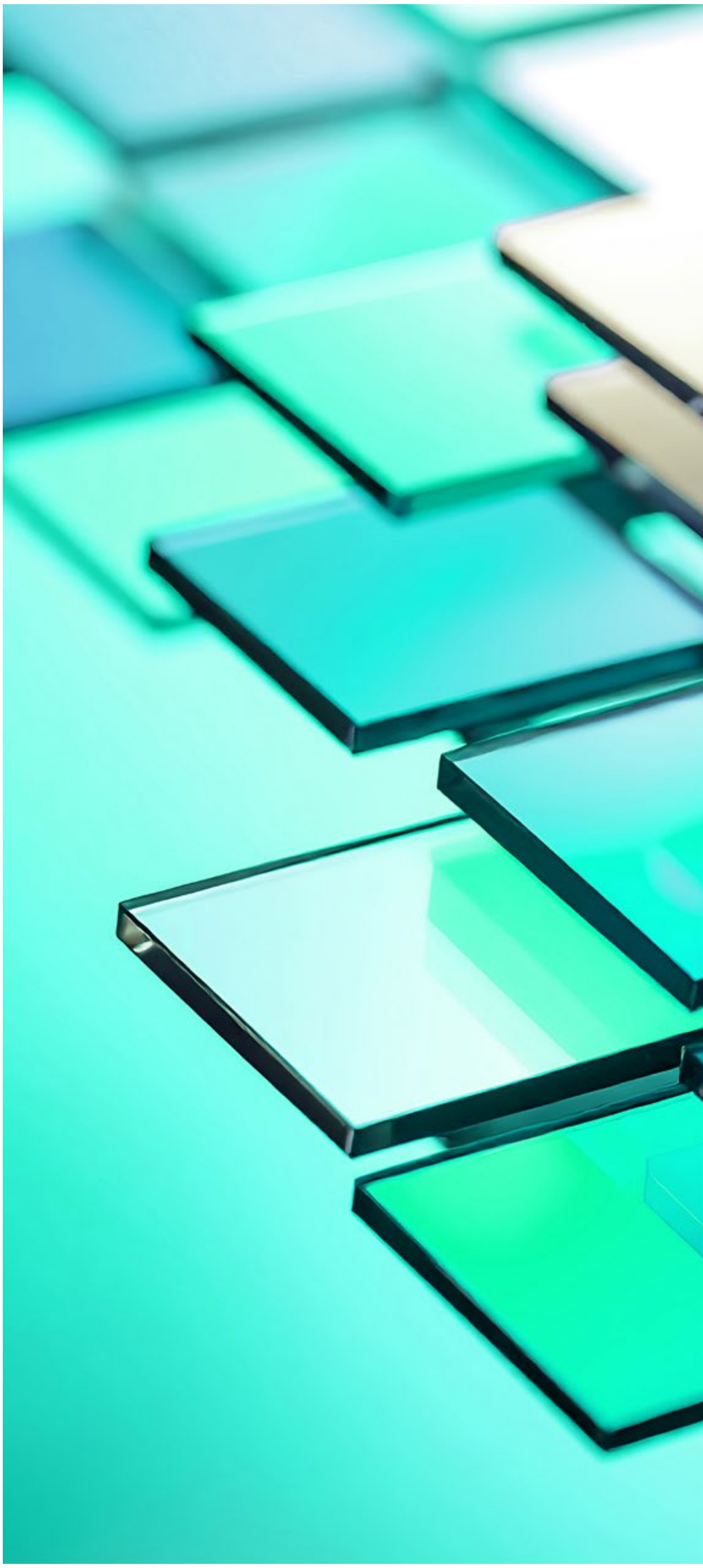
FUJIFILM Value from Innovation | IT Services

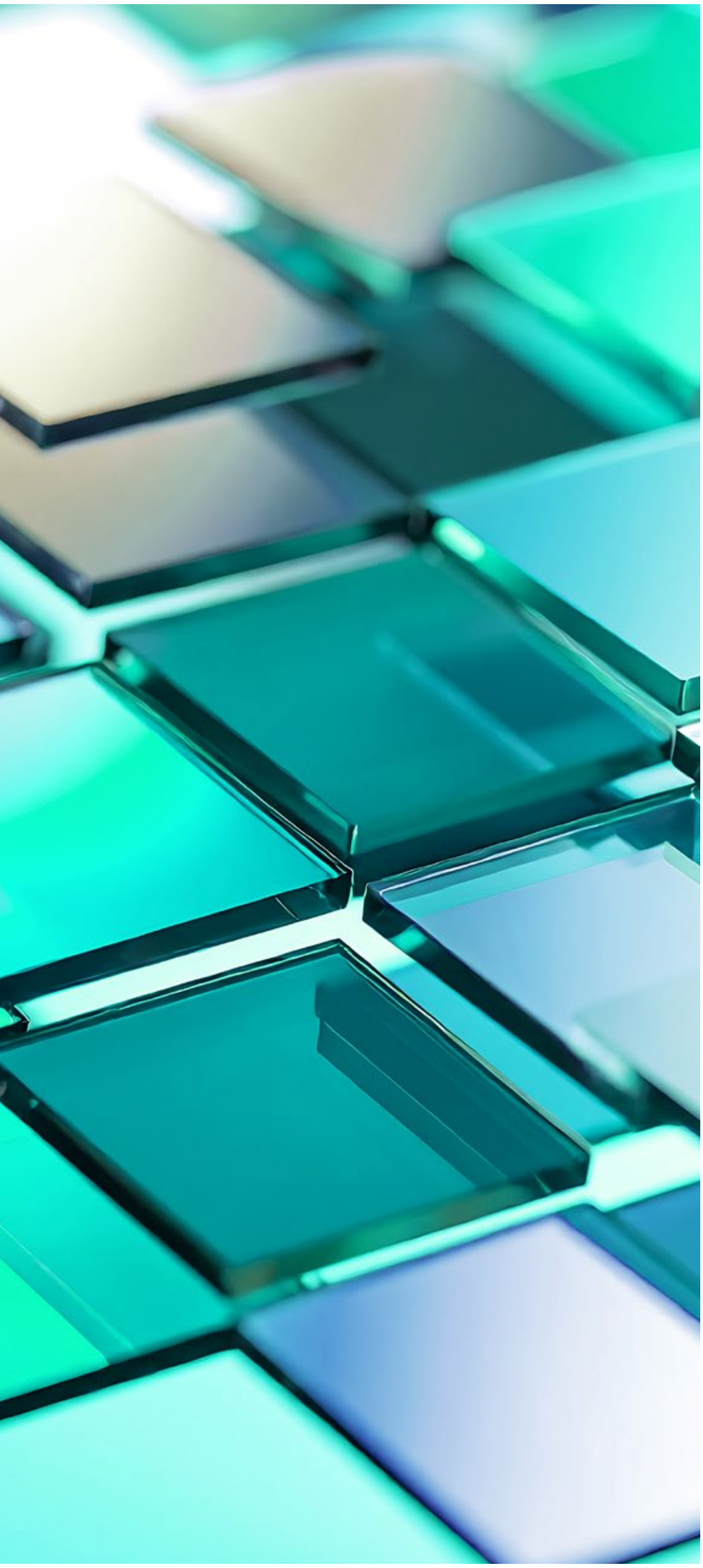


The Cyber Resilience Imperative

A Leadership Guide to Understanding Your Cyber Maturity

Table of Contents





Introduction

Cybersecurity Has Become a Leadership Responsibility

Cybersecurity has moved beyond the domain of technical specialists and IT teams. Today, it sits firmly within the sphere of executive leadership, risk governance and organisational resilience.

In an increasingly digital economy, cyber risk is no longer simply an operational concern. It is a strategic issue capable of affecting revenue, regulatory compliance, operational continuity and organisational reputation. A single cyber incident can disrupt operations, expose sensitive information and undermine stakeholder trust in ways that may take years to rebuild.

Across Australia, cyber incidents continue to rise in both frequency and sophistication. According to the Australian Cyber Security Centre (ACSC), more than **84,700 cybercrime reports were received nationally during the 2024–25 financial year — equivalent to one cybercrime reported every six minutes**. During the same period, the ACSC responded to **over 1,200 cybersecurity incidents**, reflecting an **11 percent increase year-on-year**.[1]

At the same time, organisations are undergoing rapid digital transformation. Cloud adoption, hybrid work environments, interconnected supply chains and increasing reliance on data-driven services have expanded the digital attack surface. According to the Microsoft Digital Defense Report, threat actors are increasingly targeting identity systems , cloud infrastructure and supply chains at unprecedented scale, with thousands of password-based attacks occurring every second across global networks.[2]

As a result of these developments cybersecurity has been elevated to the boardroom.

Executive leaders and directors are increasingly asking fundamental questions about organisational resilience:

- Do we understand our organisation's true cyber risk exposure?
- Are our security controls aligned with recognised best practices?
- How do we compare with organisations in our industry?
- Are we prepared to detect, respond to and recover from cyber threats?

For many organisations, the challenge is not the absence of security technologies. Firewalls, endpoint protection platforms, identity systems and monitoring tools are widely deployed across modern IT environments.

The challenge is **visibility and measurement**.

Security tools alone do not provide a clear understanding of an organisation's overall cyber resilience. Without a structured way to evaluate security capabilities across governance, technology, processes and people, leadership teams often struggle to confidently assess their cyber risk posture.

This is where **cyber maturity** becomes essential.

Cyber maturity refers to an organisation's ability to consistently manage cyber risk through structured governance, effective controls, trained personnel and resilient technology systems. It provides a framework for evaluating cybersecurity capabilities, benchmarking against recognised standards and identifying areas for improvement.

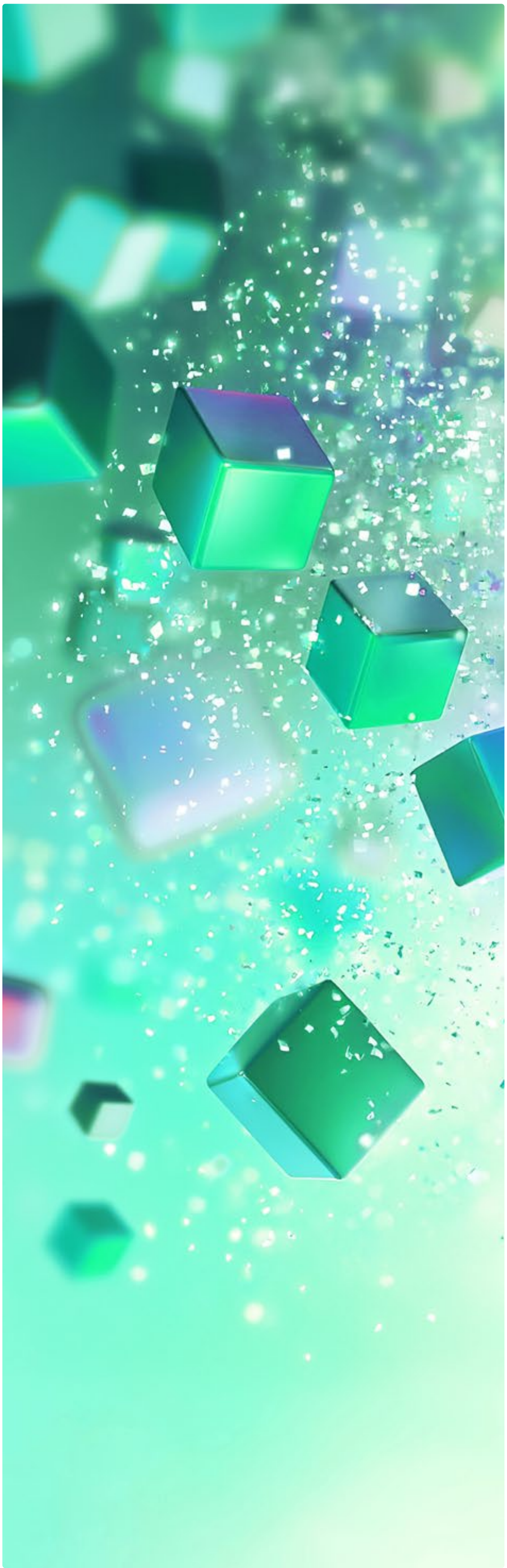
Understanding cyber maturity allows organisations to move beyond reactive security management and toward proactive **cyber resilience**.

In this guide, we explore:

- Why cyber risk has become a strategic leadership issue
- The expanding accountability for cybersecurity across organisations
- The challenges organisations face when evaluating their security posture
- The frameworks used to measure cyber maturity
- The circumstances that often trigger organisations to reassess their cyber resilience
- How independent cyber maturity assessments help organisations benchmark their capabilities and prioritise improvements

Cyber resilience is not achieved through a single technology deployment or security initiative. It is the result of **continuous evaluation, improvement and adaptation** in response to an evolving threat landscape.

For many organisations, the first step toward stronger cyber resilience is gaining a clear understanding of where they stand today.



Chapter 1

The Expanding Accountability for Cyber Risk

Historically, cybersecurity was viewed primarily as a technical discipline managed within IT departments. Security teams focused on protecting networks, maintaining perimeter defences and safeguarding systems from unauthorised access.

While these responsibilities remain essential, the scope and impact of cyber risk have evolved significantly.

Today, cyber incidents can disrupt entire organisations.

A ransomware attack can halt business operations. A compromised email account can trigger fraudulent financial transactions. A data breach can expose sensitive personal information and result in regulatory scrutiny, legal consequences and reputational damage.

These impacts extend far beyond the IT environment.

As a result, cyber risk is now widely recognised as an **enterprise risk**, comparable to financial, operational and compliance risks. Boards and executive leadership teams are increasingly expected to oversee and manage cyber resilience as part of broader organisational governance.

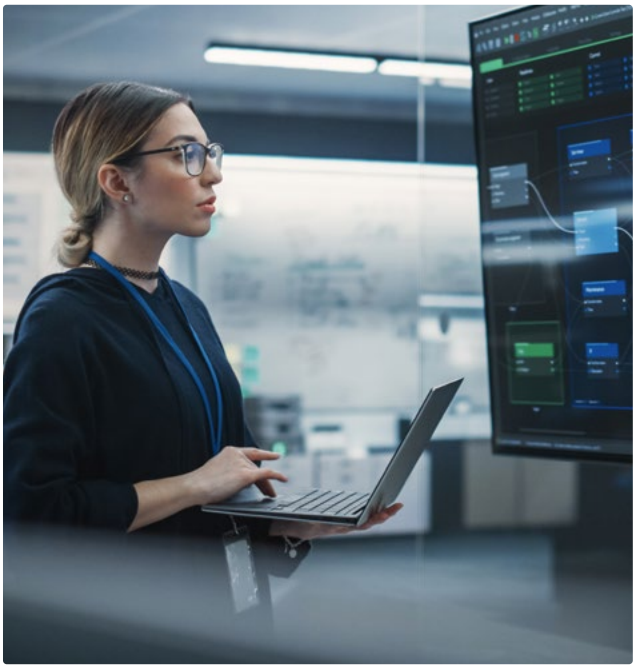
Research from Deloitte highlights that cybersecurity is now a critical, top-tier boardroom agenda item. Amidst accelerated digital transformation and an evolving, high-stakes threat landscape, global boards are actively "leaning in" to enhance their oversight of cyber risk. Leadership teams are expected to demonstrate not only that security technologies are deployed, but that cyber risks are actively measured, managed and communicated at an executive level.

This shift has changed the expectations placed on technology leaders.

Chief Information Officers (CIOs), Chief Information Security Officers (CISOs) and Heads of IT must now translate technical vulnerabilities into business risks. They are responsible for helping executive stakeholders understand potential impacts and guiding investment decisions that strengthen cyber resilience.

At the same time, cybersecurity requires collaboration across multiple functions.

Cyber resilience depends not only on technology but also on governance, processes and human behaviour. Responsibility therefore extends across the organisation, including:



— Technology Teams

Responsible for infrastructure and security controls.

— Risk and Compliance Leaders

Responsible for governance and regulatory alignment.

— Finance Leaders

Responsible for assessing financial exposure and investment priorities.

— Human Resources Teams

Responsible for security awareness and training.

— Executive Leadership

Responsible for setting organisational direction and accountability.

Cybersecurity is no longer confined to the IT department. It has become a **shared leadership responsibility** across the organisation.

Despite this increased focus, many organisations still lack a clear evidence-based view of their overall cyber resilience.

Security controls may exist and technologies may be deployed, but without a structured method of evaluating security capability, organisations often lack a clear understanding of their overall resilience against modern threats.

This uncertainty highlights the importance of cyber maturity frameworks and independent assessments, which provide organisations with a structured way to evaluate capabilities, benchmark against recognised standards and prioritise improvements that strengthen long-term cyber resilience.

Chapter 2

Five Moments That Reveal Your Cyber Risk

For many organisations, cybersecurity improvements do not begin with a long-term strategic roadmap. Instead, they are triggered by specific events such as a security incident, audit finding, regulatory change, cyber insurance requirements, or the introduction of new digital systems, that reveal potential weaknesses in an organisation's security posture.

These moments often prompt leadership teams to pause and ask an important question:

Do we really understand our cyber risk?

In many cases, the answer is unclear.

While organisations may have invested in security technologies and policies, these trigger events often highlight gaps in visibility, governance or preparedness. As a result, organisations increasingly turn to structured cyber maturity assessments to better understand their capabilities and identify areas for improvement.

The following scenarios represent some of the most common situations that prompt organisations to evaluate their cyber maturity.

1. When the Board Starts Asking Cyber Questions

Cybersecurity is now a regular agenda item for many boards and executive committees.

Directors are increasingly aware that cyber incidents can disrupt operations, damage reputations and create regulatory consequences. As a result, boards are asking management teams to demonstrate that cyber risks are being effectively managed.

Typical questions from boards include:

- How exposed are we to cyber threats?
- How do our security capabilities compare with industry best practice?
- Are we adequately prepared to respond to a cyber incident?
- How resilient are our systems and data?

Answering these questions can be challenging without a structured way to measure cybersecurity capability.

Technology leaders may have detailed knowledge of individual security tools and controls, but translating this information into a clear picture of organisational resilience is often difficult. A cyber maturity assessment provides an independent, framework-based evaluation that helps organisations communicate their security posture to executive leadership and board stakeholders.

2. Preparing for Compliance, Certification or Cyber Insurance

Another common trigger for evaluating cyber maturity is the need to demonstrate compliance with security standards or regulatory frameworks.

Many organisations adopt or align with recognised cybersecurity frameworks such as:

- The Australian Cyber Security Centre's Essential Eight
- ISO/IEC 27001
- NIST Cybersecurity Framework
- CIS Critical Security Controls

These frameworks provide structured guidance for strengthening cybersecurity practices. However, organisations often find it difficult to determine how closely their existing controls align with these frameworks.

In addition, cyber insurance providers increasingly require evidence that organisations maintain strong security practices before issuing or renewing policies. Insurers may request information about identity management, backup resilience, patch management and incident response capabilities.

A cyber maturity assessment can help organisations benchmark their existing controls against recognised standards, identify gaps and prioritise remediation efforts.

3. After a Cyber Incident or Security Scare

Many organisations reassess their cybersecurity posture following a security incident.

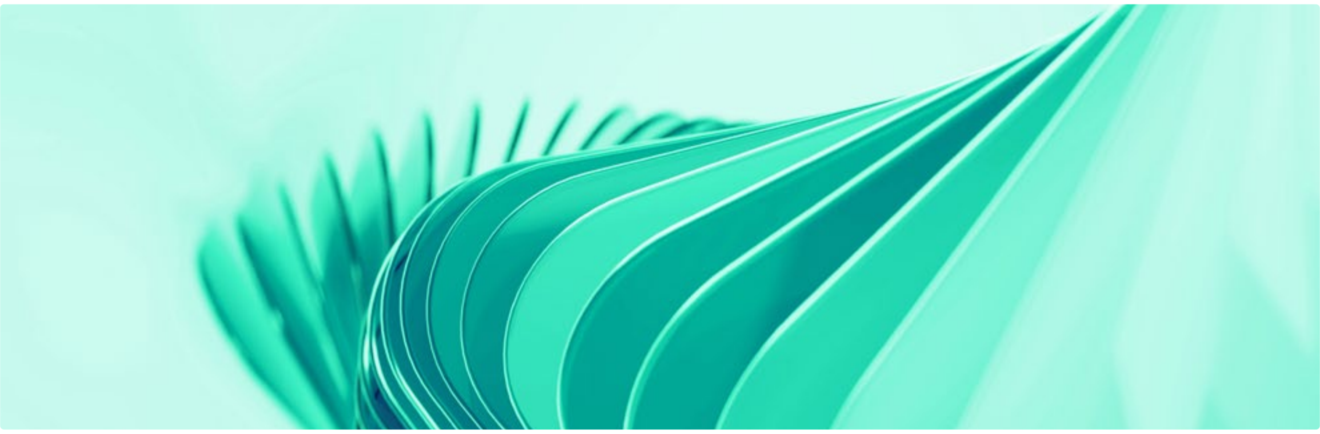
These incidents do not always involve large-scale breaches. In many cases, they begin with seemingly minor events such as:

- A phishing email successfully compromising an employee account
- Suspicious login activity detected within cloud systems
- Malware discovered on a workstation
- A supplier experiencing a security breach that affects shared systems or data

Even when these incidents are quickly contained, they often highlight weaknesses in security controls, cyber defence capabilities or incident response processes.

According to the Australian Cyber Security Centre, ransomware and business email compromise remain among the most common cyber threats affecting Australian organisations. These incidents frequently expose gaps in identity security, monitoring capabilities or user awareness.

Following such events, leadership teams often seek a clearer understanding of their overall cybersecurity posture and whether additional vulnerabilities may exist elsewhere within their technology environment , processes or organisational controls.



4. Digital Transformation Expands the Attack Surface

Digital transformation initiatives can significantly increase organisational exposure to cyber threats.

As organisations adopt cloud platforms, remote working technologies and interconnected applications, their technology environments become more complex and distributed. While these changes deliver productivity and innovation benefits, they also introduce new security challenges.

Common examples include:

- Cloud platforms that require new identity and access management controls
- Hybrid work environments that expand endpoint exposure
- SaaS applications that introduce additional data governance considerations
- Integration between systems that creates new potential attack paths

The Microsoft Digital Defense Report highlights that identity-based attacks and credential compromise have become one of the most common methods used by cyber attackers to gain access to corporate environments.

Organisations undergoing digital transformation often recognise that their existing security controls were designed for traditional on-premise environments. As infrastructure evolves, security strategies must evolve alongside it.

Cyber maturity assessments help organisations evaluate whether their security practices have kept pace with technological change and hybrid work environments.

5. Preparing for Future Cyber Resilience

In some cases, organisations proactively seek to strengthen their cybersecurity posture before a major event occurs.

Rather than waiting for an incident or regulatory requirement, forward-thinking organisations recognise that cyber resilience is an ongoing capability that must evolve alongside business growth and technological change.

These organisations often aim to:

- Benchmark their security capabilities against recognised frameworks
- Identify vulnerabilities before they can be exploited
- Prioritise cybersecurity investments more effectively
- Demonstrate strong governance and risk management practices

Independent cyber maturity assessments provide a structured way to evaluate current capabilities and build a roadmap for continuous improvement.

Moving From Uncertainty to Visibility

Each of these scenarios highlights the same underlying challenge: **organisations often lack a clear and objective understanding of their cyber maturity**.

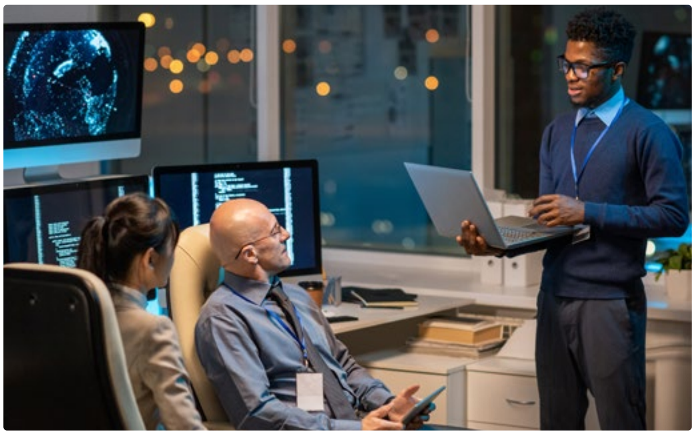
Security technologies may be deployed and policies may exist, but without a structured assessment framework it can be difficult to determine how effectively these controls operate together to protect the organisation.

Cyber maturity assessments help address this challenge by providing a comprehensive evaluation of cybersecurity capabilities across governance, technology, processes and people.

By establishing a baseline of current capability, organisations can move from uncertainty toward clear, evidence-based visibility into their cyber resilience.

Chapter 3

Why Organisations Struggle to Understand Their Cyber Posture



For most organisations, cybersecurity investments have increased significantly over the past decade. Firewalls, endpoint protection platforms, identity management systems and threat monitoring tools are now common components of modern IT environments.

Yet despite these investments, many leadership teams still find it difficult to confidently answer a fundamental question: **How secure are we today?**

Understanding cyber risk is far more complex than simply deploying security technologies. True cyber resilience depends on the interaction of governance, people, processes and technology operating together effectively.

Without a structured framework for evaluating these components, organisations often struggle to gain a clear and comprehensive view of their security posture.

Several factors contribute to this challenge.

Security Tools Do Not Equal Security Maturity

Modern organisations typically operate dozens of security technologies across their IT environments. These tools may include endpoint protection platforms, vulnerability scanners, identity management systems, security monitoring solutions and data protection tools.

While each of these technologies plays an important role, they do not automatically provide a holistic view of cyber resilience.

Security tools often operate in isolation, producing technical alerts and operational data that can be difficult to translate into meaningful business insights. Leadership teams may know which tools are deployed, but this does not necessarily indicate how effectively those tools are configured, integrated or managed.

In many cases, organisations equate technology deployment with security maturity, when in reality maturity depends on how well controls are implemented, monitored and continuously improved.

Complex Technology Environments

The rapid evolution of digital technology has significantly increased the complexity of IT environments.

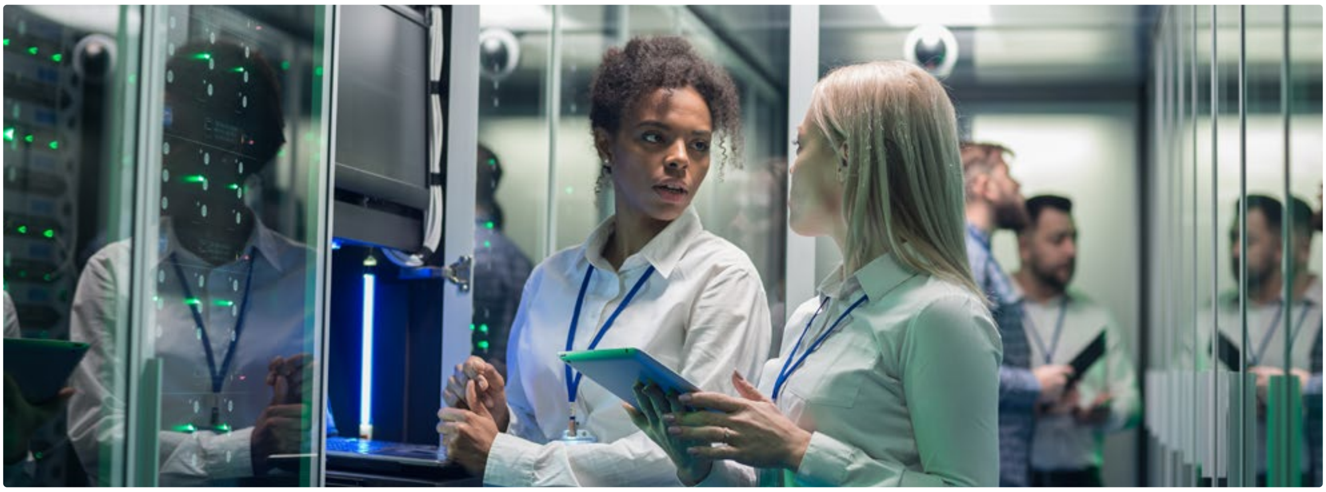
Many organisations now operate across a combination of:

- On-premise infrastructure
- Cloud platforms
- Software-as-a-Service applications
- Remote and hybrid work environments
- Connected partner and supplier systems

This complexity creates new opportunities for cyber attackers to exploit misconfigurations, weak access controls or unmonitored systems.

The Microsoft Digital Defense Report highlights that identity-based attacks and credential compromise have become one of the most common attack methods used by cyber criminals to gain access to corporate systems. These attacks often exploit gaps in authentication controls, access management or monitoring capabilities.

As technology ecosystems expand, maintaining consistent security controls across all environments becomes increasingly challenging.



Limited Visibility Across the Organisation

Cybersecurity risks rarely exist within a single system or department. They often emerge from interactions between multiple technologies, processes and user behaviours.

For example:

- An employee may reuse passwords across multiple systems
- A cloud service may be configured incorrectly
- A third-party supplier may introduce a vulnerability through system integration
- A critical system may lack effective monitoring or logging

These types of issues are difficult to identify without comprehensive visibility across the entire technology environment.

According to the IBM Cost of a Data Breach Report 2025, organisations that are able to detect and contain breaches quickly experience significantly lower financial impacts compared with those that lack effective monitoring and response capabilities. This highlights the importance of visibility and coordination across security systems.

Cybersecurity Is Not Only a Technology Challenge

Another reason organisations struggle to understand their cyber posture is that cybersecurity extends far beyond technology.

Effective cyber resilience depends on multiple organisational factors, including:

- Governance and risk management frameworks
- Security policies and procedures
- Employee awareness and training
- Incident response planning
- Vendor and supply chain security practices

Weakness in any one of these areas can create vulnerabilities that attackers may exploit.

For example, a highly sophisticated security platform may still be ineffective if employees are unaware of phishing risks, if incident response procedures are unclear, or if privileged access controls are poorly managed.

Cybersecurity maturity therefore requires coordination across the entire organisation.

The Challenge of Measuring Cyber Resilience

Because cybersecurity spans technology, governance and human behaviour, measuring cyber resilience can be difficult without a structured framework.

Organisations may track individual security metrics such as vulnerability counts, patching performance or security alerts. While these metrics are valuable, they rarely provide a comprehensive view of organisational resilience.

Leadership teams often need a broader perspective that answers questions such as:

- Are our cybersecurity capabilities aligned with recognised industry standards?
- Which areas of our security program are strongest?
- Where do the greatest risks or vulnerabilities exist?
- How should we prioritise investment to improve resilience?

Without a consistent method of measurement, it can be difficult to answer these questions with confidence.

This is why many organisations are increasingly turning to cyber maturity frameworks.

These frameworks provide structured models for evaluating cybersecurity capabilities, benchmarking against recognised standards and identifying areas for improvement.

By using a maturity-based approach, organisations can move beyond fragmented security metrics and gain a clearer understanding of their overall cyber resilience.

Chapter 4

What Cyber Maturity Looks Like in Practice

Cyber maturity is often discussed in theoretical terms, but in practice it reflects how consistently an organisation can anticipate, withstand and recover from cyber threats.

Highly mature organisations are not defined by a single technology or security control. Instead, they demonstrate a consistent ability to manage cyber risk across governance, operations and technology.

Cyber maturity therefore represents a progression in how organisations approach cybersecurity.

Early-stage programs are typically reactive, focusing on responding to incidents and implementing individual security controls. As maturity increases, organisations move toward more structured governance, proactive threat management and integrated security capabilities.

Understanding this progression helps leadership teams identify where their organisation currently sits and what improvements will deliver the greatest impact.

R

Reactive Security

At the early stages of maturity, cybersecurity is largely reactive.

Security initiatives are often implemented in response to specific incidents, compliance requirements or emerging threats. Controls may exist, but they are typically deployed in isolation and managed within individual teams.

Common characteristics include:

- Security tools implemented independently rather than as part of a coordinated strategy
- Limited visibility into how security controls operate across the organisation
- Incident response processes that are informal or inconsistently applied
- Security governance that is primarily driven by IT rather than executive leadership

Many organisations begin their cybersecurity journey in this stage, particularly as digital infrastructure evolves rapidly.

Managed Security

As organisations mature, cybersecurity becomes more structured and coordinated.

Security policies, procedures and governance frameworks are established to ensure controls are implemented consistently across systems and teams. Security programs begin to align with recognised frameworks and risk management practices.

Characteristics of this stage often include:

- Formal cybersecurity policies and governance structures
- Defined incident response procedures and testing exercises
- Centralised monitoring of security alerts and events
- Regular vulnerability management and patching programs
- Security awareness training for employees

At this stage, organisations are actively managing cybersecurity rather than responding to incidents on an ad hoc basis.

Integrated Security

More mature organisations integrate cybersecurity into broader business operations and risk management practices.

Security capabilities become embedded across the organisation rather than operating solely within the IT function. Executive leadership and boards receive regular visibility into cyber risk exposure and resilience capabilities.

Key indicators include:

- Cyber risk incorporated into enterprise risk management frameworks
- Security controls consistently applied across infrastructure, applications and identities
- Regular security testing such as penetration testing and incident simulations
- Collaboration between technology, risk, legal and operational teams

Integrated security programs allow organisations to anticipate potential threats and respond more effectively when incidents occur.

Adaptive Cyber Resilience

At the highest levels of maturity, cybersecurity becomes a strategic capability that evolves continuously in response to emerging threats.

Security teams operate with strong visibility across the technology environment and leverage threat intelligence, automation and advanced monitoring to anticipate and respond to cyber activity.

Characteristics of highly mature organisations often include:

- Continuous monitoring and threat detection across environments
- Automated security controls and rapid incident response capabilities
- Strong identity security and privileged access management
- Regular board-level reporting on cyber risk and resilience
- Continuous improvement based on threat intelligence and lessons learned from incidents

These organisations recognise that cybersecurity is not a static program but a dynamic capability that must evolve alongside the threat landscape.

Maturity Enables Better Decision Making

Understanding cyber maturity allows leadership teams to move beyond isolated security discussions and evaluate cybersecurity capability more strategically.

Rather than focusing on individual security tools or incidents, organisations can assess how effectively their security program operates as a whole.

This perspective enables more informed decisions about where to invest, which risks require immediate attention and how security capabilities should evolve as the organisation grows.

For many organisations, achieving this level of clarity requires structured evaluation of their cybersecurity capabilities. This is where cyber maturity assessments play an important role .

Chapter 5

The Role of Independent Cyber Maturity Assessments

As organisations strengthen their cybersecurity capabilities, many reach a point where internal visibility alone is no longer sufficient to fully evaluate cyber resilience.

Security teams typically maintain strong operational insight into their environments. They monitor vulnerabilities, track patching performance, manage identity systems and respond to security alerts on a daily basis. However, translating these operational insights into a clear, organisation-wide view of cyber maturity can be challenging.

Cyber maturity assessments provide a structured approach for evaluating cybersecurity capabilities across governance, technology, processes and people. By examining how these elements interact across the organisation, assessments provide leadership teams with a clearer understanding of how effectively cyber risk is being managed.

Importantly, these assessments focus not only on the presence of security controls, but also on how consistently and effectively those controls operate across the environment.

Establishing an Objective Baseline

One of the primary benefits of a cyber maturity assessment is the establishment of an objective baseline.

Security programs often evolve over time in response to new technologies, emerging threats and regulatory requirements. As a result, organisations may have strong security capabilities in some areas while other areas remain less mature.

A maturity assessment evaluates cybersecurity capability against recognised frameworks and best practices, helping organisations understand their current level of maturity and where improvements may be required.

This baseline allows leadership teams to move beyond assumptions and gain a clearer picture of their current security posture.

Benchmarking Against Recognised Standards

Cyber maturity assessments also enable organisations to benchmark their capabilities against recognised frameworks and industry standards.

Frameworks such as the Essential Eight, NIST Cybersecurity Framework and ISO 27001 provide widely accepted reference points for evaluating cybersecurity programs. Assessments translate these frameworks into practical evaluations that identify how closely current security practices align with recommended controls and governance models.

This benchmarking provides valuable context for leadership teams, enabling them to understand how their cybersecurity capabilities compare with established best practices.

Supporting Governance and Board Visibility

Cybersecurity has become an increasingly important topic for boards and executive leadership teams. Directors are expected to understand how cyber risks could affect the organisation and whether appropriate safeguards are in place to mitigate those risks.

Cyber maturity assessments help translate technical security practices into insights that are more accessible to executive stakeholders. Assessment outcomes typically provide structured reporting on cybersecurity capabilities, maturity levels and priority improvement areas.

This enables organisations to communicate cybersecurity posture more clearly within governance frameworks and provide greater transparency to boards and risk committees.

Prioritising Investment and Improvement

Cybersecurity investments can span a wide range of technologies, processes and training initiatives. Without a structured view of current capability, it can be difficult to determine which investments will have the greatest impact on organisational resilience.

Maturity assessments identify gaps across security capabilities and provide recommendations for strengthening controls over time. This allows organisations to prioritise improvement initiatives based on risk exposure and business impact rather than reacting to individual incidents.

Building a Roadmap for Cyber Resilience

Cyber resilience is not achieved through a single initiative. It is the result of continuous improvement as technology environments evolve and threat actors develop new techniques.

Cyber maturity assessments provide a foundation for this improvement by establishing a clear starting point and identifying the most effective next steps.

From this baseline, organisations can develop a structured roadmap that progressively strengthens security capabilities across governance, operations and technology.

Over time, this roadmap helps organisations move from reactive security practices toward more integrated and adaptive cyber resilience.

Conclusion

Understanding Your Cyber Maturity Is the First Step

Cybersecurity is now a core organisational risk that requires visibility at the leadership level.

As organisations adopt cloud platforms, digital services and interconnected systems, the complexity of managing cyber risk continues to increase. Maintaining resilience requires more than deploying security technologies. It requires a clear understanding of how effectively cybersecurity capabilities operate across the organisation.

Cyber maturity provides a structured way to evaluate this capability.

By assessing cybersecurity across governance, technology, processes and people, organisations gain greater visibility into their current posture and the areas where improvement will have the greatest impact.

For many organisations, the most valuable starting point is an independent cyber maturity assessment.

Assess Your Cyber Maturity

FUJIFILM IT Services provides a **Cyber Maturity Assessment** designed to help organisations evaluate their current security posture and benchmark their capabilities against recognised frameworks.

The assessment provides structured insights into cybersecurity maturity and identifies practical opportunities to strengthen cyber resilience.

Learn more about the **Cyber Maturity Assessment** here:

[1] Australian Cyber Security Centre. (2025). Annual Cyber Threat Report 2024–25. Australian Signals Directorate. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

[2] Microsoft. (2024). Microsoft Digital Defense Report. Retrieved from: https://www.microsoft.com/en-au/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[3] Deloitte. (2026). The Technology Risk Landscape – Considerations for Boards. Retrieved from: https://www.deloitte.com/uk/en/services/audit-assurance/perspectives/technology-risk-landscape.html

[4] Australian Cyber Security Centre. (2025). Annual Cyber Threat Report 2024–25. Australian Signals Directorate. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf

[5] Microsoft. (2024). Microsoft Digital Defense Report. Retrieved from: https://www.microsoft.com/en-au/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[6] PMicrosoft. (2024). Microsoft Digital Defense Report. Retrieved from: https://www.microsoft.com/en-au/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

[7] IBM. (2025). Cost of a Data Breach Report 2025. Retrieved from: https://www.ibm.com/reports/data-breach

Reference:

- Australian Cyber Security Centre. (2025). Annual Cyber Threat Report 2024–25. Australian Signals Directorate. Retrieved from: https://www.cyber.gov.au/sites/default/files/2025-10/Annual%20Cyber%20Threat%20Report%202024-25.pdf
- Microsoft. (2024). Microsoft Digital Defense Report. Retrieved from: https://www.microsoft.com/en-au/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024
- Deloitte. (2026). The Technology Risk Landscape – Considerations for Boards. Retrieved from: https://www.deloitte.com/uk/en/services/audit-assurance/perspectives/technology-risk-landscape.html
- IBM. (2025). Cost of a Data Breach Report 2025. Retrieved from: https://www.ibm.com/reports/data-breach
- Australian Cyber Security Centre. (2025). Essential Eight Maturity Model. https://www.cyber.gov.au/resources-business-and-government/essential-eight

fujifilm.com/fbau

FUJIFILM Business Innovation Australia Pty Ltd
Level 2, 54 Waterloo Road, Macquarie Park, NSW 2113 Australia
Contact us at fujifilm.com/fbau or 13 14 12