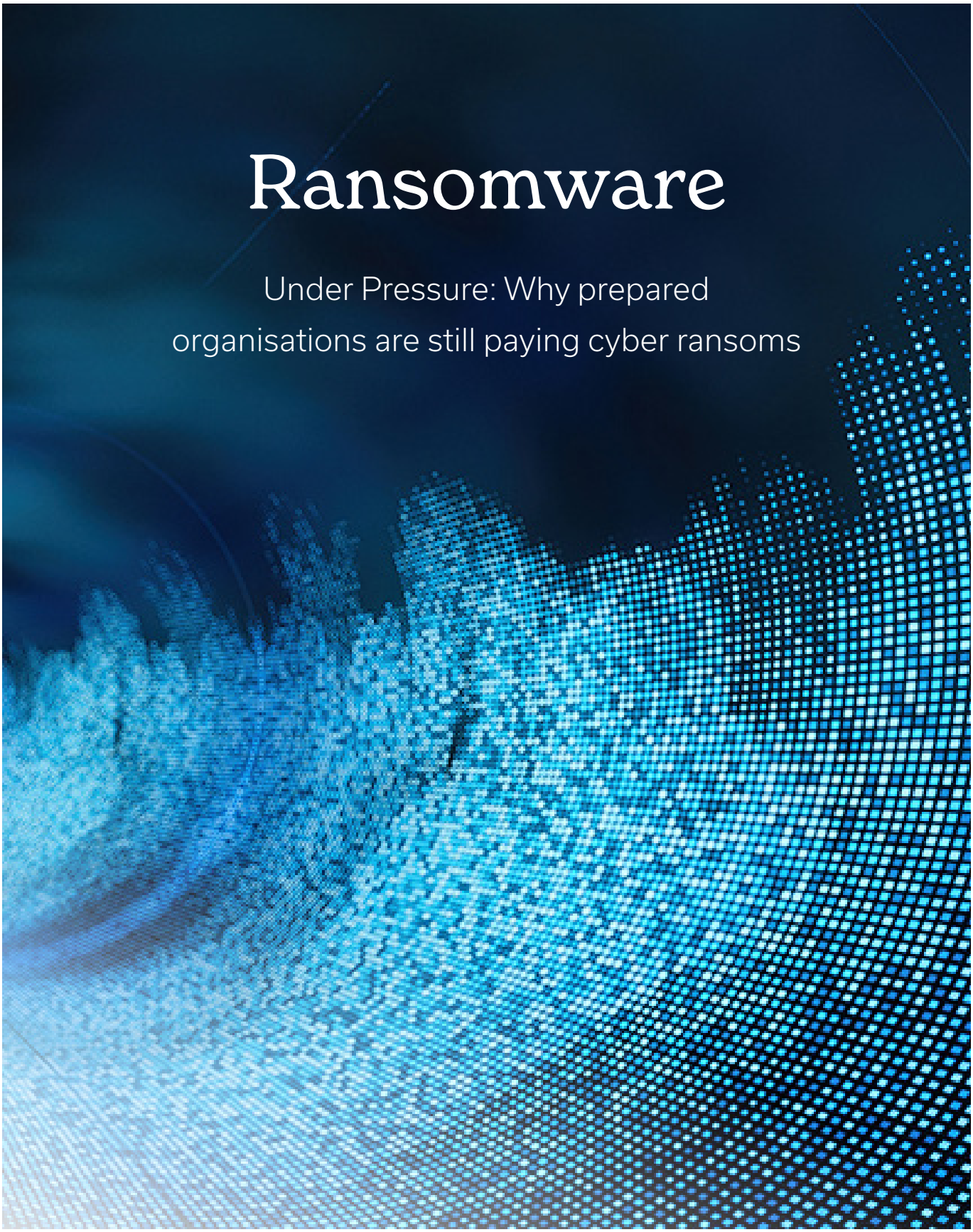
McGrathNicol

2026 RANSOMWARE REPORT

In Partnership with YouGov Australia





"It's not enough to have an incident plan, governance framework or insurance policy sitting on your desk. The real test is when an organisation is under pressure. Do these plans still hold up?"

— **Darren Hopkins**, Partner, Head of Cyber

Foreword

I am pleased to introduce the 2026 McGrathNicol Ransomware Report. Over the past six years, McGrathNicol has captured the experiences of business leaders, tracking changing attitudes towards cyber ransom payments and reporting. Ransomware continues to test the leadership of Australian organisations. As threat actors target all sectors of our economy, strengthening Australia's national cyber resilience remains a shared responsibility.

The 2026 survey presents a far more nuanced picture than a rise or fall in attack volumes. While the proportion of organisations reporting successful breaches has declined, payment behaviour has moved in the opposite direction over 12 months. More attacked businesses chose to pay a cyber ransom, payments were made faster, and negotiation became less common than in previous years.

The decisive moments occur under extreme pressure: critical systems are down, sensitive information may be at risk, customers and employees are looking for answers, and boards must make decisions with limited information available. Since we began tracking these trends in 2021, the results indicate significant investment by organisations to improve their incident response capabilities and preparedness. Australian organisations may be better equipped, but this is still not translating into confident decision-making and recovery when it matters most.

Encouraging progress has been made since the introduction of ransomware payment reporting obligations under the Cyber Security Act 2024. Awareness of the reporting framework is high. However, reputational concerns, public disclosure, legal liability and reporting complexity are cited as barriers to reporting. The findings further highlight the need to equip Australia's small and medium-sized businesses with additional skills, guidance and practical support.

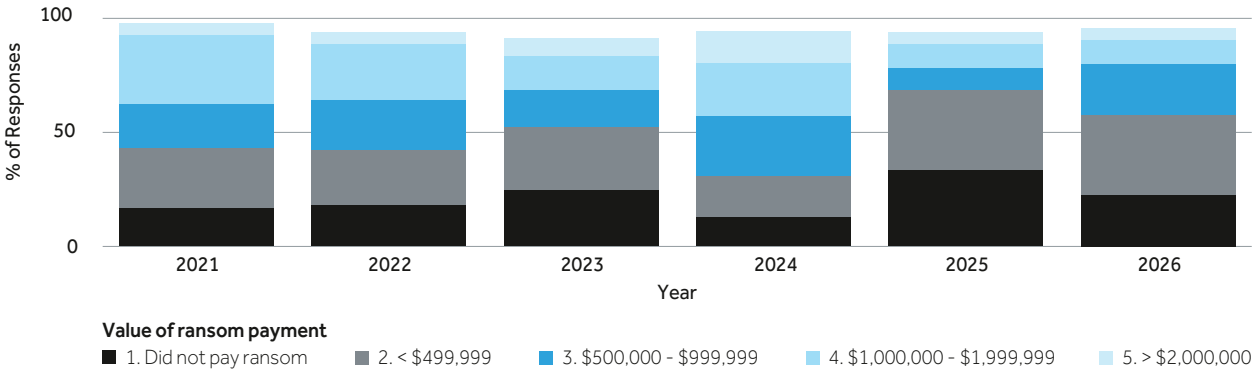
McGrathNicol's perspective is grounded in experience supporting organisations across the economy through cyber crises. We see the strain on businesses, boards, employees, customers and supply chains. This year's findings show that it is not enough to have an incident plan, governance framework or insurance policy in place. Formal plans need to be tested regularly in real life simulations, so that when an organisation is under pressure, everyone knows what to do and how to execute on those plans with confidence.



Darren Hopkins
Partner, Head of Cyber
+61 7 3333 9870
dhopkins@mcgrathnicol.com

6-YEAR TREND OF CYBER RANSOM PAYMENTS

Value of ransom payment from 2021 - 2026



Contents

Executive summary	5
The payment paradox in 2026	6
The SME resilience gap	9
Response to ransomware payment reporting	12
Ransomware lessons	14
Financial Services	16
Health & Aged Care	18
Technology	20
Five priorities for boards and executives	23
How we help	24

The numbers to know

42% of Australian businesses experienced a ransomware attack in the past 12 months. Ransomware remains an immediate and widespread threat.

30% of Australian businesses were successfully breached by ransomware in the past five years. Nearly one in three experienced an attack that resulted in a successful compromise.

38% vs 17% — Smaller businesses were more than twice as likely to be successfully breached. 38% of businesses with annual turnover below $50 million were successfully breached in the past five years, compared with 17% of businesses with turnover above $50 million.

59% of breached businesses experienced a severe or significant impact to their IT operations. For many victims, a successful breach resulted in major disruption, extended delays or operations being almost or entirely halted.

78% of businesses that fell victim to an attack ultimately paid a ransom. This increased materially from 64% in 2025, showing the continued pressure businesses face once an attack occurs.

$794,000 was the estimated average ransom payment. This increased from $711,000 in 2025, highlighting the significant financial consequences of ransomware.

Executive summary

Fewer successful breaches, faster payment decisions

The 2026 McGrathNicol Ransomware Report identifies a business environment where executives are taking active steps to increase their levels of preparedness and cyber security response. Insurance, incident response planning and board notification protocols are widespread. Awareness of reporting obligations and payment consequences also remains high.

The survey reveals a fundamental tension where most Australian organisations have the plans, insurance and governance frameworks expected of a mature cyber resilience program, but those that suffer a ransomware attack are now more likely to pay. Among organisations that paid a ransom, 40% did so within 24 hours, up 11 percentage points from 2025. As payment decision-making accelerates, organisations are becoming less likely to negotiate with threat actors to potentially delay or reduce costs. Executive confidence in perceived levels of preparedness is also softening.

This year's survey captures the views of 1,000 decision makers across Australian businesses with 50 or more employees. It was designed to reflect the current Australian business landscape, one dominated by small to medium-sized enterprises (SMEs).

More than four in five (82%) believe that SMEs are more vulnerable to ransomware attacks than larger organisations, with SME vulnerability seen as a combined people, technical expertise and funding challenge.

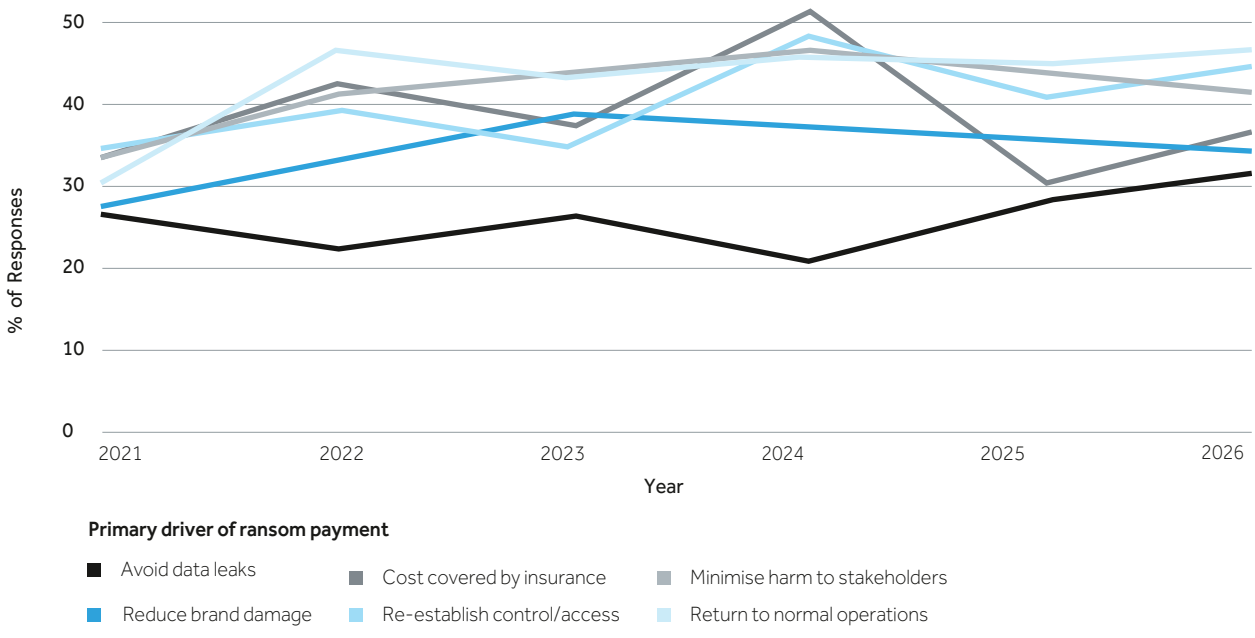
Collectively, the results suggest that Australian organisations have plans in place but aren't regularly testing their decision-making, recovery and reporting capabilities. When under pressure, organisations are making faster decisions and have reduced confidence in their formal plans.

For policy makers, there is an opportunity to move from awareness to practical, incident-ready guidance. Scenario-based materials may help to explain reporting triggers, timelines and responsibilities, while reporting processes could be adapted to reflect the reality of the first 24 hours of an incident.

For business leaders, the priority is to test whether internal teams, critical suppliers and external advisers can coordinate and act decisively against a realistic ransomware scenario. When time and information are constrained, formal plans must be clear so that everyone knows what to do and who to call in the event of a real crisis.

6-YEAR TREND OF PRIMARY DRIVERS BEHIND RANSOM PAYMENTS

Breakdown of primary drivers from 2021 - 2026



The payment paradox in 2026

NUMBER TO KNOW

84% of businesses say they would be willing to pay a cyber ransom (up from 81% in 2025).

Despite investment in preparedness, insurance and response planning, attack rates remain high and ransomware continues to pose significant operational, financial and reputational challenges. While successful breaches and repeat attacks have declined compared with 2025, a greater proportion of businesses are paying, and they are paying more quickly.

McGrathNicol's Cyber team has seen these patterns in recent incidents. The data reflects the reality of managing a crisis, where payment decisions are often considered before an organisation has gathered reliable evidence about data access, recovery time, threat actor attribution and credibility. Under pressure, organisations tend to prioritise business continuity at all costs. In 2026, 88% of business leaders consider their organisation prepared to respond to a cyber attack. While this remains a high level of confidence, it is down from 96% in 2025, suggesting Australian organisations may be taking a slightly more measured view of the challenges in responding to a ransomware attack in practice.

Organisations are making faster payment decisions and negotiation is becoming less common

Of the organisations that experienced an attack in the past five years and decided to pay a ransom, two in five (41%) decided not to negotiate before paying (up from 31% in 2025). Based on McGrathNicol's experience supporting SMEs through ransomware incidents, a lack of technical expertise and dedicated cyber security personnel, combined with funding constraints, are likely reasons. Smaller organisations are often unable to access specialist incident response and threat actor negotiation when critical decisions need to be made. This can result in payment being viewed as the fastest path to restoring operations, without first testing whether the amount can be reduced or if alternative recovery options are available.

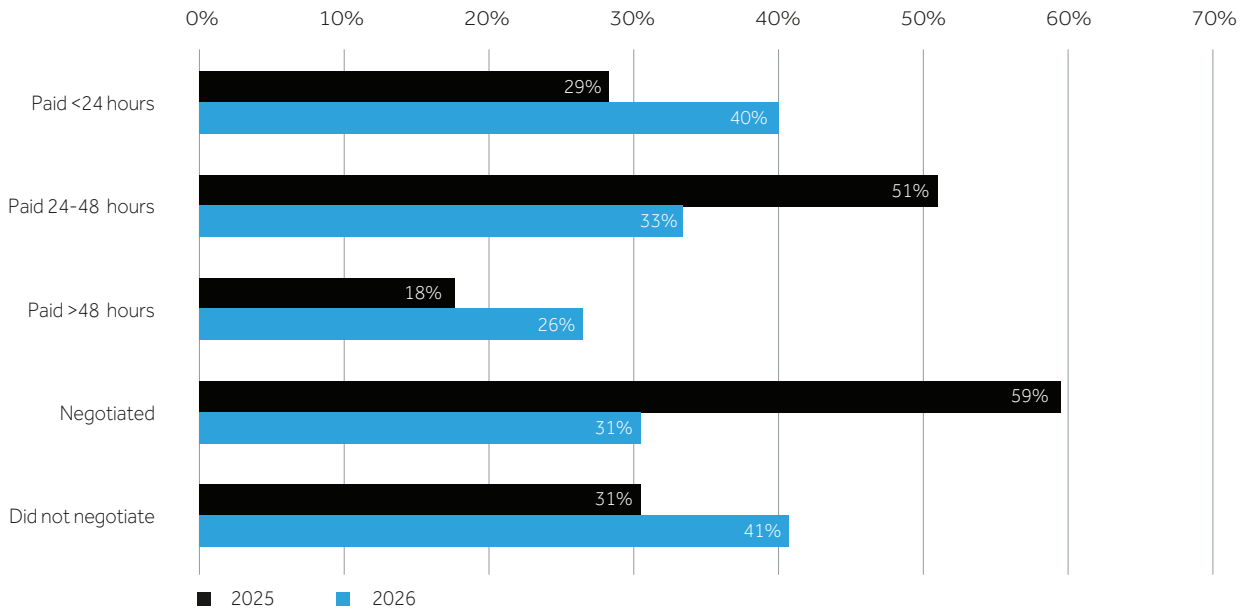
While the average payment amount of $794,000 represents an increase from 2025, this is below historical records. Insurance prevalence remains high at 93%, but the average coverage amount of $960,000 has continued to decline since 2024.

Most Australian businesses remain willing to pay

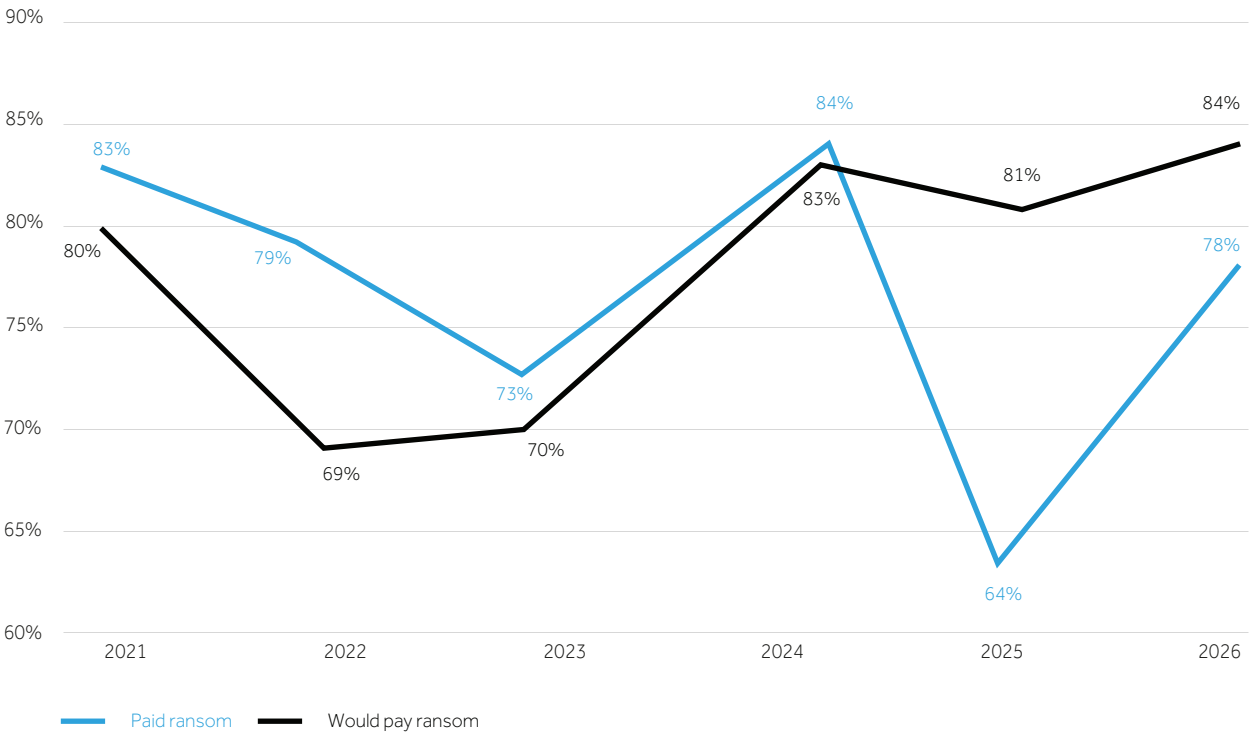
The average estimated amount of $850,000 that executives say they would be willing to pay is down from $906,000 in 2025, and follows a YoY declining trend. The most cited reasons for paying a ransom relate to operational recovery, including getting back to normal operations faster (46%), re-establishing control of critical systems (43%) and minimising harm to employees, customers and suppliers (42%). More than three quarters (76%) identify at least one risk-related driver for paying a ransom, while 69% identify at least one operational driver.

Nearly nine in ten (87%) executives are aware that paying a ransom helps fund criminal organisations. This illustrates the value of ongoing collaboration and information sharing between government and industry, and represents growing awareness and education,

FASTER PAYMENTS COINCIDE WITH LESS NEGOTIATION



PAYMENT APPETITE AND WILLINGNESS INCREASES





"When ransomware creates material operational or data risk, no matter the size of the organisation, executives face powerful pressures to pay."

— **Brendan Payne,** Partner

The SME resilience gap

NUMBER TO KNOW

82% believe that SMEs are more vulnerable to ransomware attacks than larger organisations.

Australia's business landscape is predominantly made up of small businesses, making the ransomware vulnerability of SMEs a broader economic resilience issue. More than four in five business leaders (82%) believe SMEs are more vulnerable to ransomware than larger organisations, citing a lack of dedicated cyber security personnel (37%), limited technical expertise (35%) and constrained cyber security budgets (35%) as limitations.

The survey highlights a significant resilience gap for smaller Australian businesses. While smaller businesses are not necessarily experiencing more ransomware attacks, the findings indicate they are more susceptible to successful compromise. Businesses with annual turnover below $50 million were more than twice as likely to have been successfully breached over the past five years as businesses with turnover above $50 million, (38% compared with 17%).

This finding reinforces the Australian Government's focus on small and medium businesses under Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. For smaller businesses, the challenge is not simply reducing the likelihood of being targeted. It is building the capability to prevent an attempted attack from becoming a successful breach, and to respond and recover quickly when preventative controls fail.

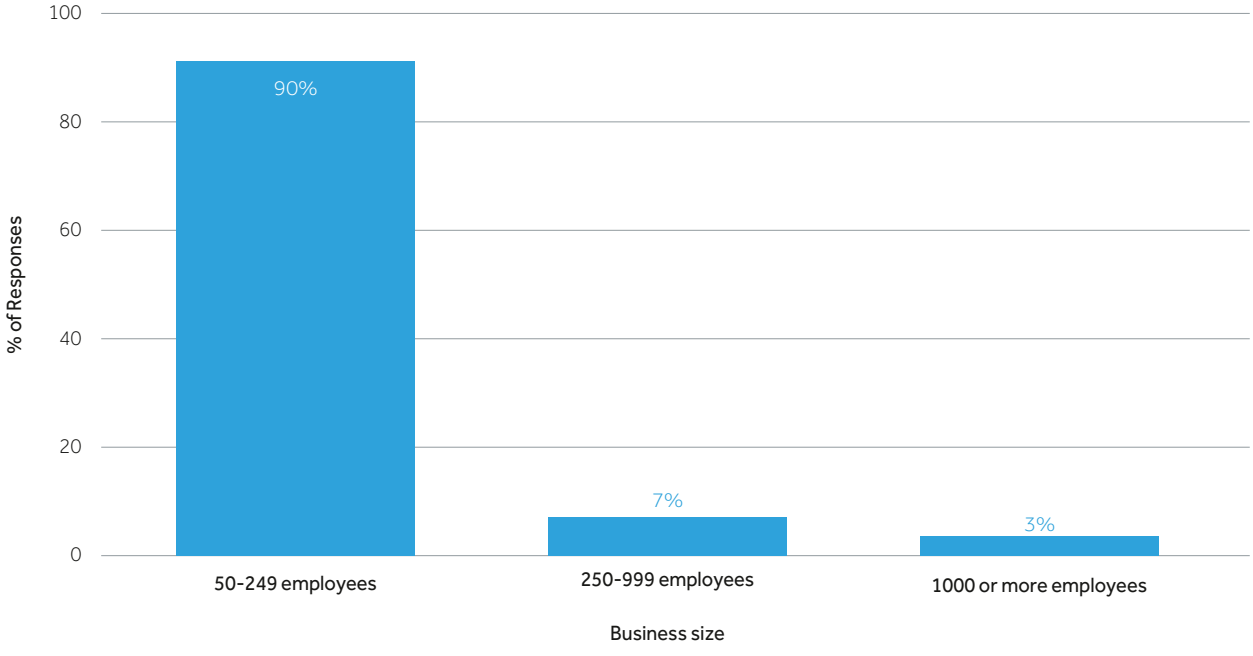
Why SMEs are more vulnerable to ransomware

- Limited incident response planning and recovery capability can make a ransom payment seem like the fastest route to restoring operations.
- An SME may have appropriate technology but lack a dedicated person to interpret threat alerts, coordinate suppliers and make informed risk decisions.
- Greater reliance on third parties, such as suppliers and outsourced providers, can create uncertainty about who holds the evidence, who can isolate systems, and who is authorised to communicate with government, insurers and customers.

This is consistent with McGrathNicol's frontline experience, as smaller organisations often require access to a coordinated external response team spanning forensics, insurer engagement, legal, communications, and ongoing data recovery support.

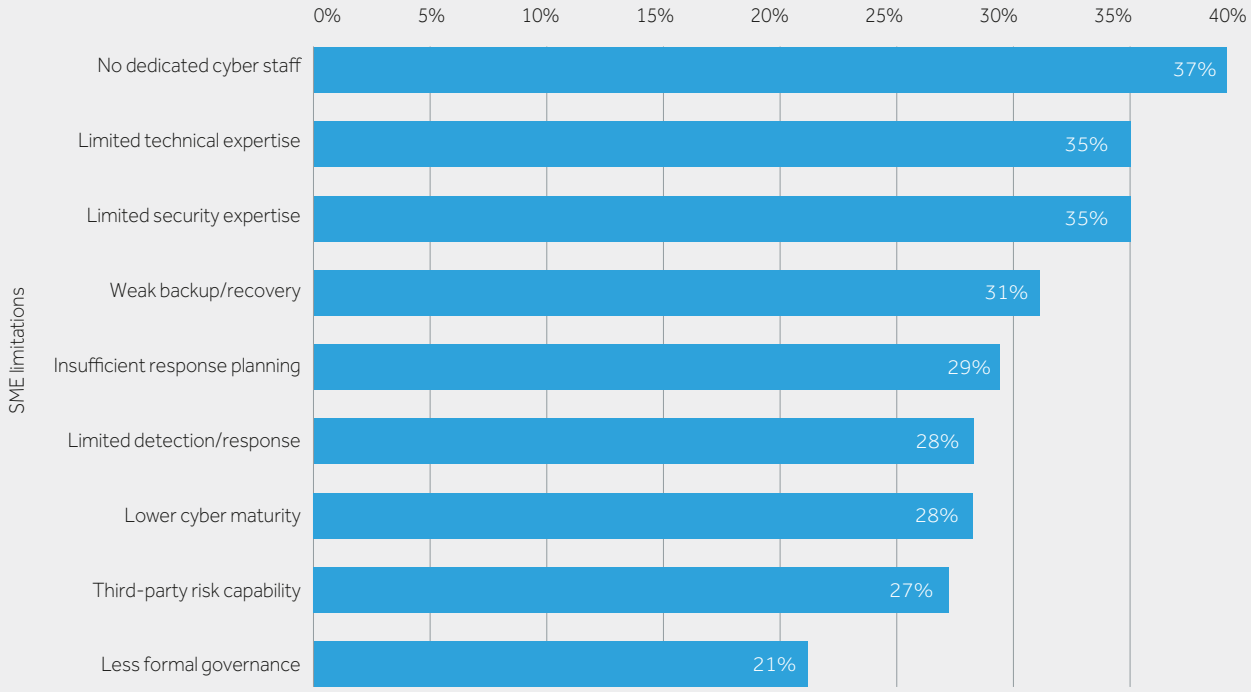
BUSINESS SIZE VS RANSOMWARE ATTACKS

Businesses that experienced a ransomware attack in the past 12 months



THE SME RESILIENCE GAP STARTS WITH PEOPLE AND EXPERTISE

The most significant cyber security capability gaps affecting SMEs



SME resilience starts with knowing who to call

Our experience conducting security assessments, cyber resilience reviews, incident response engagements and cyber exercises across small and medium-sized Australian businesses, not-for-profit organisations and other entities indicates that cyber maturity challenges are broadly consistent across this group.

Low cyber maturity is rarely the result of organisational indifference or a lack of care toward cyber risk. There is strong motivation and intent to drive cyber risk management and maturity, but this is constrained by competing priorities, reduced budgets, limited access to cyber expertise, uncertainty regarding what needs to be done, and difficulty navigating an increasingly complex cyber security landscape.

Many organisations do not have dedicated cyber security personnel and instead rely on internal IT teams, outsourced technology providers, or operational staff to manage cyber security responsibilities alongside their primary role. In smaller organisations, responsibility for cyber security frequently sits with executives, finance teams, operations managers or owners who have limited formal cyber security training.

The most effective resilience measure for many SMEs is establishing trusted external support well before an incident occurs. Organisations that know who to call, what decisions need to be made, and how they will recover will be better positioned to avoid rushed payment decisions and restore operations with confidence.

Steps to build resilience before a crisis

1. **Rehearse the payment decision before you need to make it**
   Many organisations spend time planning technical recovery but never discuss how they would approach a ransom demand. Boards and executives should agree decision rights, escalation processes, insurer engagement, legal considerations and the information required before a payment decision is considered. The objective is not to decide whether you would pay, but to understand how that decision would be made under pressure.
2. **Pre-agree reporting obligations and responsibilities under the Cyber Security Act 2024**
   The first 24 hours of a ransomware incident are often chaotic. Organisations should identify who is responsible for assessing reporting triggers, liaising with legal advisers, engaging regulators and coordinating notifications under the Cyber Security Act 2024. Reporting should become part of the incident response process rather than a separate compliance activity.
3. **Establish your incident response team before an incident occurs**
   Organisations should maintain a pre-approved panel of advisers, including cyber incident responders, legal counsel, cyber insurers, crisis communications advisers and forensic specialists. Knowing who to call can save valuable time when systems are offline and decisions are time critical.
4. **Clarify roles, ownership and authority**
   Organisations should clearly define who has authority to engage with threat actors, approve external communications, contact customers and regulators, authorise expenditure and direct recovery activities.
5. **Test recovery without assuming the attacker will help**
   Recovery plans should be tested on the assumption that decryption keys will never be provided, even if a payment is made. Organisations should regularly validate backups, critical business processes, identity recovery procedures and manual workarounds to understand how operations would continue during a prolonged disruption.
6. **Exercise realistic ransomware scenarios**
   Tabletop exercises should include executive teams, board representatives, legal advisers and key third parties. Scenarios should include data theft, system encryption, media scrutiny, customer notifications and reporting obligations. The goal is to identify gaps before a real incident exposes them.

> "Where an organisation has no practical fallback arrangements, manual workarounds or tested business continuity processes, they may be unable to resume critical operations quickly, and in more severe cases, unable to recover at all."
>
> — **Darren Hopkins,** Partner, Head of Cyber

Response to ransomware payment reporting

NUMBER TO KNOW

92% of business leaders are aware of Australia's ransomware payment reporting obligations.

Following the introduction of ransomware payment reporting obligations under the Cyber Security Act 2024, most Australian business leaders are aware of their reporting obligations. However, less than a third (30%) describe themselves as "very familiar", 42% as "somewhat familiar", and 20% as "aware but do not know the details". Those who have an incident response plan for a cyber attack are also more likely than those that do not to be familiar with the legal reporting requirements (95% compared to 78%).

Regardless of whether a ransom payment is made, Australian businesses remain in favour of reporting: more than half (54%) believe ransomware attacks should be reported regardless of whether a ransom payment is made. Nearly three quarters (74%) believe some form of ransomware attack should be mandatorily reported to authorities.

There are opportunities to improve participation in reporting by addressing concerns relating to public disclosure, legal liability, reputational impact and reporting complexity.

The McGrathNicol annual survey has consistently shown SMEs are vulnerable to ransomware attacks, meaning there is an opportunity to capture a more accurate and complete snapshot of the threat landscape. The $3 million annual turnover threshold currently exempts many Australian SMEs from reporting ransomware payments. Expanding the legislation would enable the government and industry to better share real-time learnings with SMEs, support them in protecting and responding to attacks, and would ensure the ransomware payment reporting framework continues to deliver helpful and actionable intelligence.

Reporting expectations vs reality

Australian business leaders expect it would take 29.5 hours on average to accurately report a successful ransomware attack, with that estimate almost doubling from 17.2 hours in 2025. This reflects that business leaders potentially have more experience and/or a better understanding of the challenges in reporting a ransomware attack.

The expected assessment and reporting time among businesses without direct attack experience (29.5 hours on average) is higher than the actual average reported by businesses that experienced a ransomware attack (23.7 hours).

Horizon 2: Strengthening SME cyber resilience

The Australian Government's Action Plan for Horizon 2 of the 2023–2030 Australian Cyber Security Strategy sets out the next phase of Australia's national cyber security strategy. Covering 2026–2028, Horizon 2 moves from strengthening foundational protections under Horizon 1 to scaling cyber maturity across the Australian economy, society and digital infrastructure. It includes 19 actions delivered through 64 initiatives, with small and medium businesses specifically identified as an important part of Australia's broader cyber resilience.

Government and industry have a shared challenge

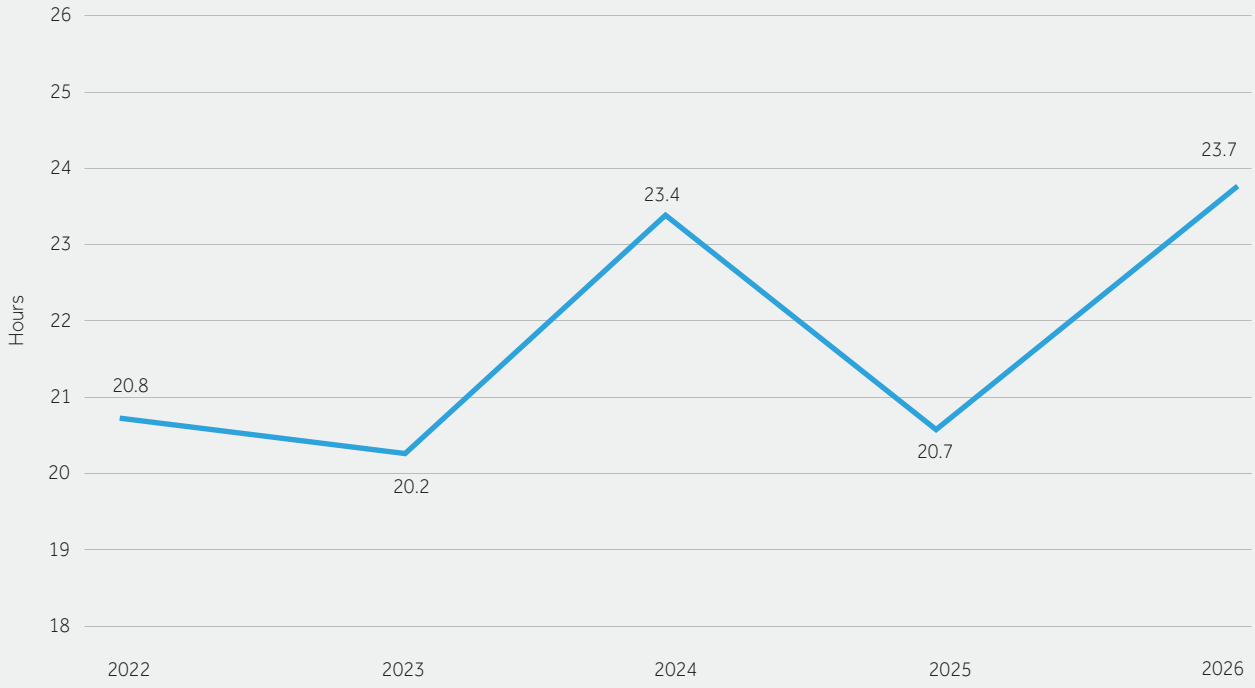
The Federal Government recognises that smaller organisations need practical and accessible support. Initiatives under Horizon 2 include the Ransomware Playbook, which provides guidance on preparing for, responding to and recovering from ransomware; the Cyber Health Check Tool, which provides a basic cyber security assessment and practical steps for improvement; and the Small Business Cyber Resilience Service, delivered through IDCARE, which provides free incident support, cyber first aid, wellbeing support and independent cyber security and privacy assistance.

Mandatory Reporting under the Cyber Security Act 2024 (Cth)

- Mandatory to report ransomware payments for businesses with annual turnover of more than $3 million or critical-infrastructure entities
- Report must be submitted within 72 hours of becoming aware of the payment, and lodged via the Australian Cyber Security Centre (ACSC) portal
- Applies to any payment including money, cryptocurrency, or non-monetary benefit (e.g. providing access credentials, data, or services). Failure to report may result in civil penalties (up to 60 penalty units per contravention)

ACTUAL ASSESSMENT TIME IS DRIFTING UPWARD AGAIN

How long it took for businesses to assess and accurately report an attack



Ransomware lessons

McGrathNicol's incident response work over the past 12 months has highlighted that threat actors are changing the tools they use, how quickly they are adapting, where they are applying pressure, and how they are seeking to control engagement during an attack. These insights are drawn from anonymised engagements and do not identify any client, victim organisation or threat actor.

CASE STUDY A —

AI is accelerating the attack lifecycle

Threat actors are using AI-enabled tools, data analysis and reasoning to support attacks. This does not necessarily mean an autonomous AI system is conducting the intrusion, but rather that AI is being used to augment human actors by helping them process information, identify opportunities and adapt faster.

What we are seeing

- In one ransomware incident, the attacker rapidly analysed the compromised environment after gaining access and adapted its approach as it identified more effective opportunities to exfiltrate data and disrupt operations. The significance was the speed and agility with which information from the environment was converted into attack decisions.
- Jason Clinton, Deputy CISO of Anthropic, spoke at the AISA CyberCon 2026 conference on October 16, 2026. He noted the industry faces a critical 18 month to 2 year window as AI systems rapidly evolve and uncover software vulnerabilities at scale. He also warned organisations to prepare for monthly large-scale cyber attacks over the coming year.

The resilience lesson

- Organisations should assume the time between access, discovery, exfiltration and disruption will compress. Early containment, identity controls, high-quality logging, rapid forensic triage and pre-agreed authority become even more important.

CASE STUDY B —

Operational technology (OT) is a deliberate disruption target

If OT can be identified and accessed, threat actors may target it because they understand the operational and commercial leverage created by disruption. OT should not be treated as incidental to an enterprise ransomware event.

What we are seeing

- In an incident, the threat actor deliberately targeted accessible OT systems to increase disruption. The actor later referred to the OT impact in communications, using the operational consequences as leverage to intensify pressure.

The resilience lesson

- Organisations with OT should plan for a combined IT and operational crisis. Asset visibility, segmentation, remote access, recovery dependencies and decision rights across IT and OT should be tested together.

CASE STUDY C —

Threat actors are forcing engagement

Threat actors are less willing to wait while an organisation decides whether to communicate. They may manufacture urgency by contacting employees or other people connected to the victim.

What we are seeing

- Across multiple ransomware matters, McGrathNicol observed threat actors reaching beyond the designated communication channel and contacting staff or people connected with the affected organisation. The apparent purpose was to provoke engagement and create additional pressure on decision-makers.

The resilience lesson

- Communications planning should account for direct threat-actor contact. Organisations need clear internal instructions, escalation channels, evidence-preservation steps and coordinated handling across executive, legal, communications, HR and security teams.

The operational lesson

Modern ransomware response requires organisations to manage a faster, more adaptive adversary across technology, operations and communications. The most resilient organisations contain threats quickly, protect critical operations, and maintain control of threat actor engagement under pressure.

Industry breakdown

Financial Services

THE NUMBERS TO KNOW

- 86% say they are prepared to respond to a cyber attack.
- 83% assessed and reported an attack within one day, compared to 70% overall.

Financial Services organisations are at comparatively high ransomware risk and are willing to pay cyber ransoms, quickly and subject to negotiation.

Highly regulated, operationally mature, and still willing to pay

Despite being one of the most cyber mature sectors, Financial Services organisations are frequently breached and payment appetite remains high. This year's survey revealed that 75% of financial services organisations reported an attack in the past five years (versus 69% overall), while 38% had been successfully breached (compared with 30%). Among breached organisations, phishing was the primary entry method.

Financial Services organisations are more willing to make a payment following a ransomware attack, reflecting the urgent need to restore access to financial systems, customer services and sensitive information. Among organisations that fell victim to an attack in the past five years, 84% chose to pay a ransom within a median payment timeframe of 24-48 hours. Three quarters (75%) of Financial Services organisations say they would be willing to pay (compared to 64% across all sectors), at an average of approximately $956,000.

The highest of any sector, financial services organisations were more likely to negotiate prior to making a ransom payment (68% versus 59% across sectors), balancing the need to mitigate financial losses with restoring critical systems, and protecting and providing information to customers and stakeholders.

Financial Services reports the fastest reporting and response times

Established governance and regulatory obligations have had a positive effect, with the sector demonstrating operational maturity in incident assessment time and reporting. Financial Services organisations are comparatively the fastest to assess and report incidents: 83% of attacked organisations completed the process within one day, well above the 70% average.

Generally, most organisations (86%) consider themselves prepared for an attack and 79% have an incident-response plan in place. The results reveal a governance gap when it comes to board-notification arrangements, however: while 83% would notify the board, this is below the 92% average across sectors. Further, only 68% of organisations have an established notification protocol compared with 77% overall.

The operational consequences of a successful breach are wide-ranging. Among breached organisations, 65% experienced a severe or significant IT impact and 67% reported a severe or significant supply chain impact. As a sector, Financial Services combines elevated breach and payment risk with relatively fast incident response times.

The main opportunity is to convert this operational readiness into stronger board escalation and easy to understand, rehearsed processes so that ransom payments are no longer considered a viable path to recovery.

Non-Bank Lender

A non-bank lender and financial services provider experienced a significant cyber incident after a threat actor obtained access to credentials associated with a cloud service account in its Amazon Web Services (AWS) environment. The threat actor used the compromised credentials to conduct reconnaissance, access cloud-hosted data repositories, create additional accounts and move laterally in an apparent attempt to maintain access. Analysis identified evidence of data exfiltration from multiple cloud storage repositories, while limitations in available logging meant the full extent of access could not be conclusively determined.

As the investigation progressed, the organisation faced increasing pressure from customers, regulators, and other stakeholders seeking assurance that the incident had been contained and that sensitive information was protected. At the same time, the organisation needed to investigate the compromise, understand the extent of unauthorised access and data exfiltration, strengthen security controls, continue business operations, and manage ongoing stakeholder communications.

What made the difference

- **Early detection and rapid response:** The organisation identified suspicious activity through existing security monitoring and promptly activated its incident response process, helping to contain the threat before further access could be established.
- **Engaging specialist expertise:** Cyber insurance and legal counsel enabled the rapid deployment of an integrated team of forensic investigators, legal advisers, cloud providers and cyber incident response specialists, ensuring multiple workstreams could proceed simultaneously.
- **Strong collaboration with technology partners:** Close engagement with AWS and third-party responders supported the validation of findings, containment of malicious activity and implementation of additional security controls across the environment.
- **Acting decisively on containment and remediation:** Access tokens and credentials were revoked, permissions reduced, additional monitoring and alerting implemented, IP restrictions enforced and security controls strengthened to reduce the likelihood of recurrence.
- **Transparency and stakeholder management:** The organisation worked proactively with advisers to provide updates and assurance to customers, investors and regulators while continuing to investigate the incident and refine its understanding of the data impact.

The lesson

Cloud security starts with understanding your data and the third parties you are working with. Strong monitoring, least-privilege access, robust logging, effective stakeholder communication and the ability to rapidly mobilise specialist support can materially improve the outcome of a significant cyber incident.

Industry breakdown

Health & Aged Care

THE NUMBERS TO KNOW:

- 89% say they are prepared to respond to a cyber attack.
- 79% of organisations experienced a ransomware attack in the past five years, the highest of any industry.
- 82% of those that fell victim to an attack chose to pay a ransom, compared with 78% across all industries.

Even prepared Health & Aged Care organisations face immense pressure when patient care, resident wellbeing, clinical systems and sensitive data are at risk.

Critical services, critical decisions

Health & Aged Care organisations report strong formal cyber preparedness yet remain more likely to pay ransoms when operations are impacted. More than seven in ten organisations (79%) reported experiencing a ransomware attack within the past five years, the highest of any industry and considerably higher than the national average (69%). This suggests frequent targeting of the sector and its ongoing attractiveness to threat actors.

Formal planning is high but does not necessarily translate into rapid incident assessment: 84% have an incident-response plan, 93% are insured against ransomware and 93% would notify their board in the event of a ransomware attack. However, following an attack, only 50% assessed the required information and reported it to stakeholders within a 24-hour period, compared with 70% of respondents overall. Nearly two thirds (65%) of Health & Aged Care organisations would be willing to pay in the event of a ransomware attack, underscoring the difficult decisions the sector faces when critical services, patient care and sensitive information are at risk.

In environments where patient health outcomes, medication management, and clinical operations are impacted, the tolerance for prolonged disruption is inevitably lower than in other sectors. Health & Aged Care organisations are more likely to cite restoring access to critical systems and returning to normal operations as key considerations.

The data also points to increased exposure to modern ransomware tactics: more than three quarters (79%) have either experienced or observed double extortion activity. Health & Aged Care organisations also reported high levels of phishing activity (52%) and business email compromise (39%). Threat actors are continuing to exploit human and operational vulnerabilities as much as technical weaknesses.

When disruption isn't an option

Even highly prepared Health & Aged Care organisations face immense pressure when patient care, emergency operating systems, and sensitive data are at risk. The sector reported one of the highest rates of successful breaches and one of the highest rates of ransom payment. For organisations delivering essential services, prolonged downtime can make ransom payment a continuity of care decision as much as a cyber security one.

Australian Healthcare Provider

A healthcare provider found itself at the centre of a serious ransomware and data-extortion incident. Attackers had gained access to its environment, stolen data and encrypted a critical application server. The pressure continued after the initial attack: the organisation was named on the threat actor's dark-web leak site and stolen data was subsequently published. At the same time, the threat actor began contacting staff directly via WhatsApp, bringing the incident out of the technology environment and directly to its people.

Faced with operational disruption, potential harm from the stolen data and growing stakeholder pressure, the organisation needed to investigate the attack, keep the business operating, understand the data impact and manage its regulatory responsibilities, all at the same time.

What made the difference

- **Leadership and transparency:** Leadership treated the incident as an organisation-wide crisis, with a clear focus on recovery, business continuity and transparent communication.
- **Immediate access to expertise:** Cyber insurance gave the organisation rapid access to an integrated forensic, legal and communications team, allowing multiple aspects of the crisis to be managed in parallel.
- **Asking for help:** The organisation engaged with the National Office of Cyber Security (NOCS) and was prepared to seek external assistance when it mattered.
- **Recovery mindset:** Business continuity and recovery became central to decision-making, including rebuilding impacted technology where necessary.
- **Knowing their data:** The organisation was able to quickly understand the affected data and its potential impact. This demonstrated the importance of data governance and gave the legal team the information needed to support required notifications.

The lesson

Cyber resilience requires strong leadership, transparency, knowing your data, asking for help and maintaining a relentless focus on recovery. These factors can materially change the outcome of any major cyber incident.

Industry breakdown

Technology

THE NUMBERS TO KNOW

- The average ransom paid by Technology organisations was approximately $1.41 million, almost double the $793,735 average.
- 88% of those that fell victim to an attack in the past five years paid the ransom, compared with 78% across all industries.
- 34% cited the need to prevent sensitive information from being leaked as a key payment driver.

Despite good intentions and very high levels of preparedness, when faced with the reality of an attack, most Technology organisations are choosing to pay to minimise harm and protect their sensitive data.

Technology organisations face elevated ransomware exposure, with 72% having experienced an attack in the past five years. Of those, 37% were successfully breached. These findings sit higher than the overall averages of other industries at 69% and 30%, respectively. Threat actors are using different modes of entry too: phishing attacks are less commonly reported (30% as opposed to 44%), while Business Email Compromise attacks are slightly higher (39% compared to 33%).

As expected, the Technology sector demonstrates very strong incident response readiness. Most organisations (93%) consider themselves prepared for a cyber attack, including 54% who report being "very prepared", higher than the average (39%). When it comes to formal planning documents and processes, 87% have an incident response plan, 86% have established a formal board-notification protocol, and 98% are covered by cyber insurance. Given the urgent nature of an attack and need for real-time intelligence sharing, the sector achieves fast incident assessment and reporting. Among Technology organisations that have experienced an attack, 83% assessed and reported the information to relevant stakeholders within 24 hours, compared with 70% overall; and almost half (43%) completed this process within seven to 12 hours.

A propensity to pay

High levels of confidence and formal preparedness are not translating to reduced payment outcomes. Technology organisations are among the most likely to pay a ransom and are paying the highest average amount.

When attacked, 88% of organisations chose to make a ransom payment and 14% paid between $2 million and $5 million—higher than the overall figure of 4%. More telling, nine in ten (89%) organisations say they would be willing to pay in the event of an attack. The research suggests Technology organisations have reached their payment ceiling though. The amount organisations say they would be willing to pay is close to the actual average amount being paid out: $1.32 million compared to $1.41 million.

Harm minimisation outweighs operational drivers

Almost half (41%) of Technology organisations cite minimising harm to employees, customers and suppliers as a consideration during payment decisions. This suggests that many understand their role within broader supply chains and the flow-on impacts, with almost all escalating an attack to Board level (98%). Risk-related considerations, such as preventing sensitive data or IP being leaked, were cited more frequently than operational drivers.

Harm minimisation sits at the forefront of boards and executives' minds. Despite many having formal plans and processes in place, these are not being regularly tested in practice with clearly assigned roles and responsibilities. Almost a third (29%) consider a ransom payment cheaper or faster than full recovery, suggesting a lack confidence in recovery capability across the sector.

Managed Service Providers

Across a number of ransomware incidents, we have seen a recurring theme: organisations have outsourced significant responsibility for their technology and security to managed service providers (MSP), but have limited visibility of how those services are being delivered.

In some incidents, the MSP itself was compromised, creating a pathway into client environments. In others, vulnerabilities remained unpatched, security alerts that could have provided an opportunity to intervene were missed, or backup and recovery environments failed when they were most needed. Threat actors were also able to target or disrupt the very systems organisations were relying on to recover.

Common observations

- **Trust without verification:** Organisations often assumed their MSP was managing security effectively, without clearly understanding how key controls were being operated or tested.
- **Unclear accountability:** Where the same provider was responsible for both IT operations and security, responsibility for identifying and escalating security issues was not always clear.
- **Missed opportunities to intervene:** Patching gaps and security alerts were not always addressed quickly enough, allowing an initial security issue to develop into a major incident.
- **Recovery that had not been tested under pressure:** Backups existed, but their architecture, isolation or recoverability had not always been sufficiently challenged against a ransomware scenario.
- **Third-party risk gaps:** Contracts, security requirements, assurance activities and ongoing third-party risk management (TPRM) did not always reflect the level of access and dependency placed on the provider.

The lesson

Outsourcing technology does not outsource cyber risk. Organisations need to understand what their MSP is responsible for, how they demonstrate that critical controls are working, where security accountability sits, and what will happen if the provider is potentially compromised. Ongoing relationships should be built on clear accountability, independent assurance and evidence, rather than assumptions.



Five priorities for boards and executives

1. **Rehearse the payment decision**
   Pre-agree decision rights, evidence thresholds, legal and sanctions checks, insurer engagement, law-enforcement contact, reporting steps and alternatives to payment.
2. **Test recovery without assuming decryption**
   Validate restoration sequencing, identity recovery, clean-room capability, business process workarounds and the time required to recover critical services.
3. **Prepare for double extortion**
   Exercise simultaneous encryption, data theft, public-leak threats, stakeholder notification and dark-web monitoring. Payment for decryption does not resolve publication risk.
4. **Make reporting executable**
   Assign accountable owners, prepare data capture templates and integrate statutory reporting into the incident response plan rather than treating it as a separate legal task.
5. **Build decision-quality evidence quickly**
   Ensure forensic collection, logging, asset inventories, data mapping and third-party access arrangements can establish what happened, what was accessed and what recovery options are credible.

How we help

Build your cyber resilience through practice

Boards, executives and regulators increasingly expect organisations to demonstrate that incident response, crisis management and business continuity arrangements are tested.

Cyber incidents require organisations to make consequential decisions with incomplete information, under time pressure and across technical, operational, legal, privacy, communications and executive functions. Cyber exercising provides a safe and controlled environment in which your organisation can practise its response, validate existing arrangements and identify improvements before a real incident occurs.

Exercises can be aligned to relevant requirements and standards, including the Security of Critical Infrastructure Act, APRA CPS 230 and ISO 27001, as well as board, audit and insurer assurance needs.Each exercise is built around a realistic scenario and followed by practical findings and prioritised actions.

Meet governance, regulatory and assurance expectations

Demonstrate that your incident response, crisis management and business continuity arrangements are current, credible and tested.

Validate coordination across the response ecosystem

Test whether multiple function teams can work effectively with critical suppliers and external advisers. This helps confirm that escalation pathways, information flows and dependencies will operate as intended.

Prepare people to act under pressure

Build familiarity with roles, plans, decision authority and available support before a crisis occurs. Exercises can induct new leaders and responders, refresh experienced teams and strengthen working relationships across functions.

Drive continual improvement

Use evidence from each exercise to identify gaps, prioritise practical actions and strengthen plans. A structured exercise program can progressively test more complex scenarios and demonstrate improvement over time.

Our Cyber Exercising, Simulation & Readiness Services

We design an exercising approach that reflects your objectives, maturity, operating environment and available resources. This can include:

Exercise strategy and program design

Develop a sustainable exercising program that identifies the plans, teams, critical services, technologies, suppliers and other dependencies that should be tested. This may include an exercising roadmap, governance arrangements, scenario library and tools to measure improvement over time.

Executive and board exercises

Test strategic decision-making, governance, crisis leadership, escalation pathways, regulatory obligations and business impacts. These exercises help clarify the respective roles of the board, executives and operational teams when decisions must be made quickly and with incomplete or contested information.

Technical and specialist team exercises

Test operational response across incident management, forensic readiness, privacy, legal, communications, business continuity and technical recovery. Exercises can examine whether teams can coordinate effectively, preserve evidence, contain the threat, assess affected systems and data, and prioritise recovery.

Multi-entity and ecosystem exercises

Test coordination across business units, suppliers, service providers, advisers, insurers, regulators and other external stakeholders. These exercises examine how information, responsibilities, decisions and dependencies are managed when an incident extends beyond organisational boundaries.

Cyber solutions to safeguard your business

The cyber threat landscape continues to evolve rapidly. AI-enhanced attacks, cloud complexity, geopolitical uncertainty and threat actor diversification mean cybercrime is always a risk. Having helped hundreds of Australian businesses respond and recover, McGrathNicol can help you navigate any cyber situation – from reducing risk, to recovering from incidents, and designing strategies that increase organisational resilience.

Our experienced team advises on incident management, crisis communications, business continuity planning, risk assessments, policy and standards development, and up-to-date compliance with industry regulations.

We are here to help you with:

- Cyber Incident Response
  Rapid response, containment, and recovery support during cyber incidents.
- Cyber Offence, Defence & Intelligence
  Proactive security testing and threat intelligence to enhance system integrity and mitigate vulnerabilities.
- Cyber Security Expert Services
  Specialised expert analysis and forensic investigation to support regulatory or legal actions.
- Cyber Strategy & Resilience
  Develop effective strategies that align with your corporate goals and deliver valuable cyber outcomes.
- Information Security
  Manage and protect your data effectively, while leveraging it for strategic advantage.
- Sensitive Data Assessment (SDA)
  We provide AI-enabled SDAs that review large structured and unstructured datasets to identify PII connected to individuals, supporting harm assessments, regulatory compliance, and effective breach response.

Contact us

Partnering with McGrathNicol's Cyber team equips you with the cyber response and protection you need to safeguard your business, critical business assets, people and customers.

www.mcgrathnicol.com/cyber

Methodology

The 2026 McGrathNicol Ransomware Survey was conducted online between 28 August and 14 September 2026 by YouGov. The study was conducted via online survey as an ad-hoc study, targeting owners/partners, board members, and C-suites in Australian businesses with 50+ employees. The sample was comprised of 1000 respondents. The findings have been weighted by business size to reflect a target profile of 90% businesses with 50-249 employees and 10% with 250 or more employees, consistent with previous years. As the survey reflects individual perspectives, findings should be interpreted as indicative rather than definitive of organisational behaviour.

Acknowledgement

Since 2021, McGrathNicol has partnered with YouGov to develop this research, providing a consistent and robust evidence base for understanding ransomware trends across Australia. We also thank the Department of Home Affairs for its input into the development of this year's questionnaire, helping ensure the research delivers insights that support industry, government and broader collective efforts to strengthen Australia's national cyber resilience.