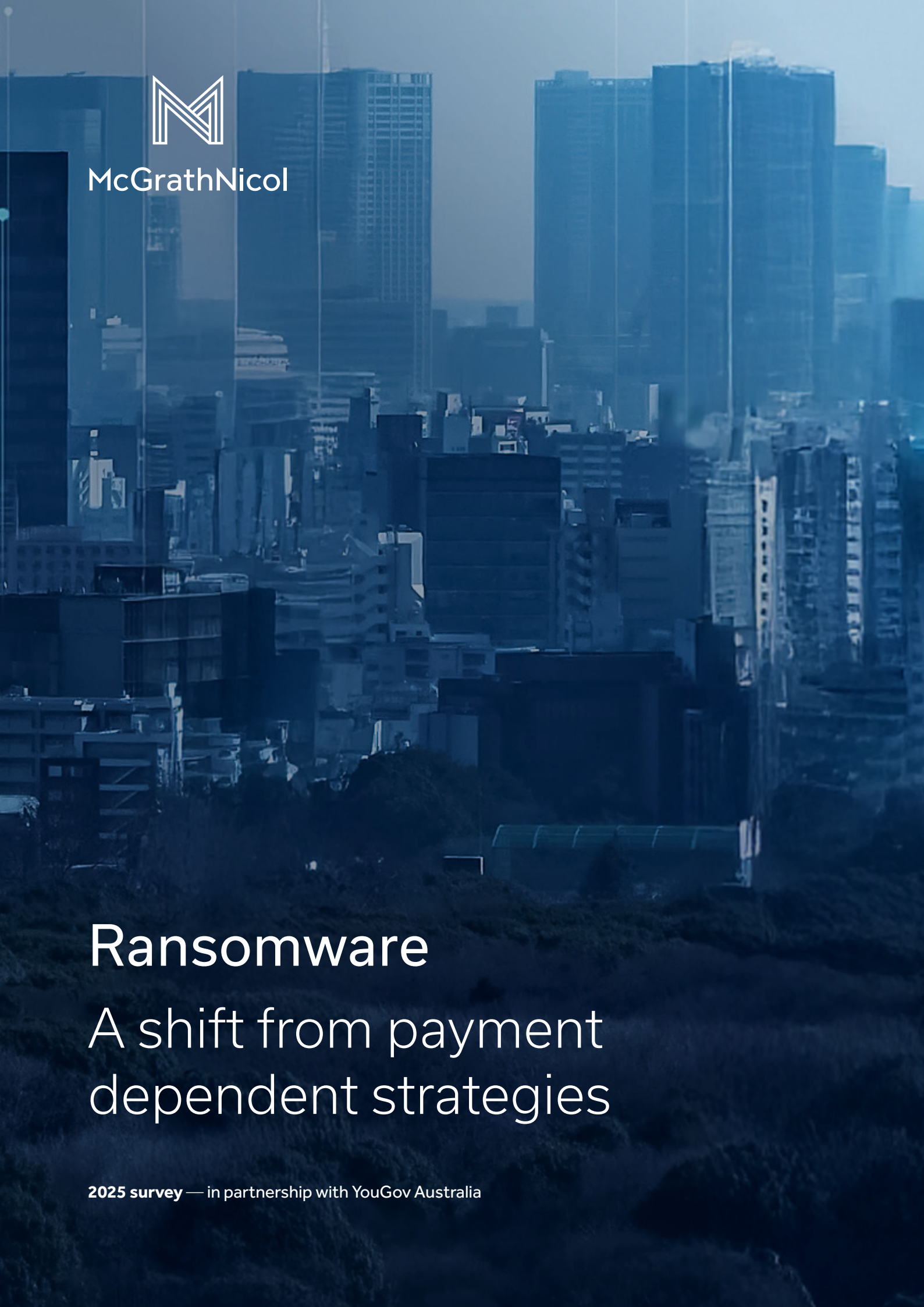


McGrathNicol

Ransomware

A shift from payment dependent strategies

2025 survey — in partnership with YouGov Australia

Contents

Foreword

I am pleased to introduce the McGrathNicol Ransomware Report for 2025. Over the past five years, the McGrathNicol Cyber team has tracked the increasing sophistication and evolution of the ransomware model. The tactics are changing, and so too are attitudes towards reporting and ransom payments.

The 2023-2030 Australian Cyber Security Strategy is already working. We are pleased to see the estimated average payment has decreased to $711,000—down from $1.35 million just 12 months ago. As ransomware attacks and data breaches increase in both scale and frequency, we are working closely with our clients, industry partners and government to share threat intelligence and respond effectively.

Small businesses continue to bear the brunt of ransomware attacks and our research underscores that most breaches and ransom payments occur in this segment. Without dedicated resources and cyber teams, many SMEs are vulnerable to being seen as "soft targets". We also know that SMEs tend to pay because they view this as their only option. This is reflected in the data, with 64% of those attacked opting to pay a cyber ransom over the past five years.

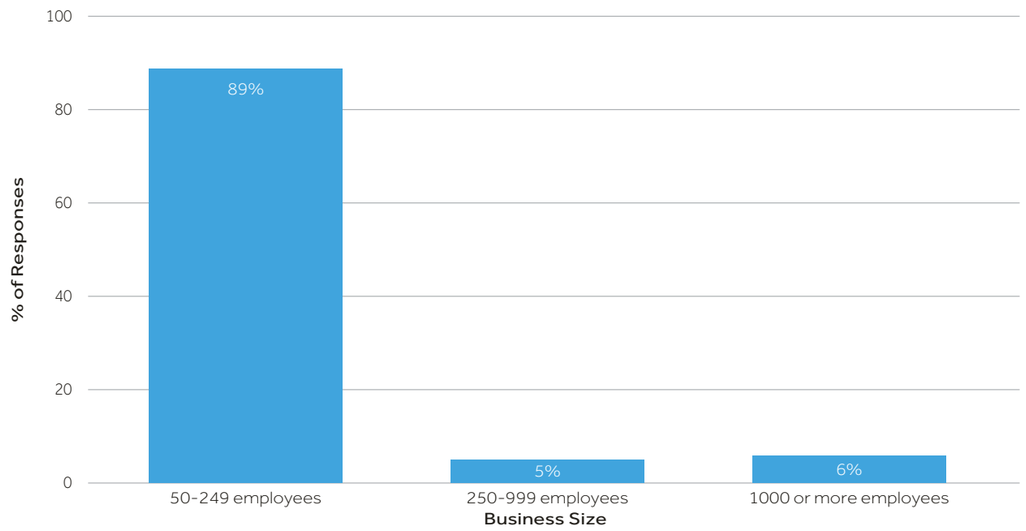
Borne out by the survey findings, there is strong business and consumer support for mandatory ransomware reporting. The aim of these legislative changes is to promote greater visibility, transparency and industry collaboration.

Encouragingly, we're seeing a shift towards proactive cyber resilience and recovery planning. Paying a ransom does not guarantee data recovery nor does it prevent future attacks.

Darren Hopkins
Head of Cyber at McGrathNicol
+61 7 3333 9870
dhopkins@mcgrathnicol.com

BUSINESS SIZE VS RANSOMWARE ATTACKS

Businesses that have experienced a ransomware attack in the past 12 months



"You can't trust cyber criminals. Minimise operational and long-term damage to your business through investment in prevention, detection, and strong incident response capabilities."

Executive Summary

Ransom Payments No Longer Seen as a 'Default Option'

The 2025 McGrathNicol Ransomware Report reveals a fundamental shift in how Australian businesses are approaching ransomware risk.

The survey included a sample of over 800 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). With 89% of organisations that have experienced an attack in the past 12 months falling within this category, the financial and operational burden on SMEs is substantial.

In positive news, the findings revealed some of the largest year-on-year changes in the study's history: the average amount that businesses say they are willing to pay has declined significantly from $1.42 million in 2024 to $906,000 in 2025. This points to a change in payment attitudes, the effectiveness of governance and reporting changes, and a shift away from payment-dependent strategies. The change also coincides with 96% of organisations feeling prepared to respond to cyber attacks—up from 93%. Almost a third (32%) of respondents say their business was able to successfully defend against an attack, which signals maturing market approaches with greater emphasis on resilience.

The survey reveals three critical payment drivers: insurance coverage amounts continue to decline, regulatory and reputational pressure is increasing; and there is growing scepticism of ransom payments as the 'default' or most viable recovery option.

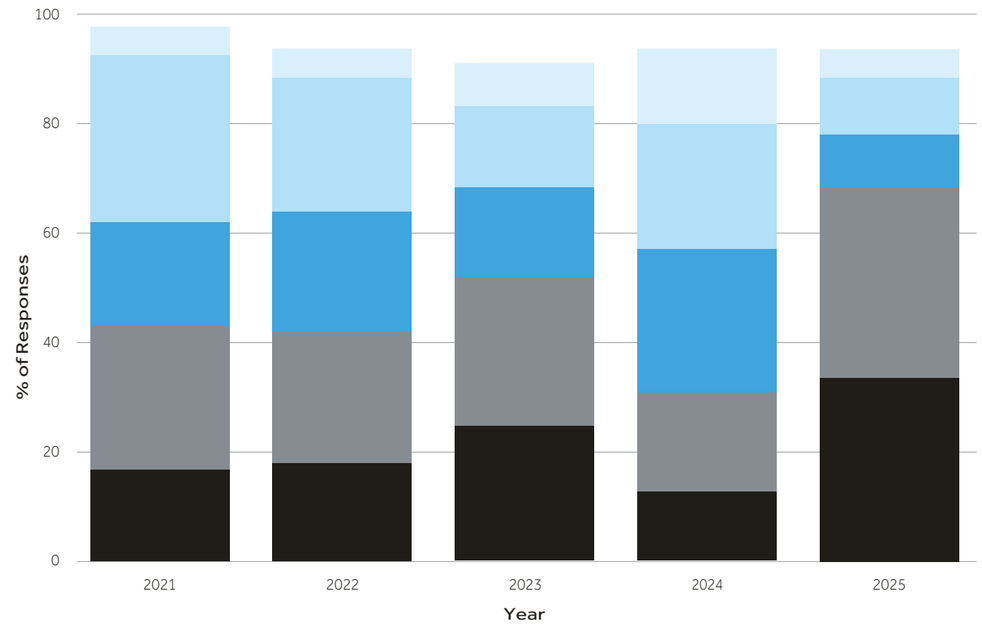
Nearly two in three (64%) say their business decided to pay a ransom, a significant decrease from previous years.

The estimated average amount of cyber ransom paid was $711,000 (down from $1.35 million in 2024).

Four in five (81%) businesses say they would be willing to pay a cyber ransom (down from 83% in 2024). One in five (20%) would only do so if there was no other choice (up from 14% in 2024).

5-YEAR TREND OF CYBER RANSOM PAYMENTS

Value of ransom payment from 2021 - 2025



Three Critical Drivers for Declining Ransomware Payments

1. The Insurance Market Catalyst

While 92% of respondents have cyber insurance in place, the nature of coverage has changed. Since 2022, the average coverage amount has declined from $1.31 million to $1.18 million. Now, more than half of organisations (54%) have coverage below $1 million, compared to 42% in 2024.

Providers have moved away from a payment-facilitating role to incentivise proactive resilience. Insurers are changing their policy structures and actively discouraging ransom payments due to unsustainable claims and regulatory pressure. The message is clear: organisations that invest in prevention and recovery capabilities will receive better terms. Organisations must focus on improving cyber security measures instead of relying on insurance to cover future ransom payments.

Cyber insurance only factored into 31% of organisations' decisions to pay, compared to 52% in 2024.

2. Regulatory & Reputational Pressure is Increasing

Regulatory scrutiny and reputational risks are creating additional pressure. Most business leaders (92%) admit that knowledge of a ransom payment would impact their perception of business partners, up from 88% in 2024. The specific concerns are evolving, with 46% worried about data security risks through networks (up from 40% in 2024) and 44% refusing to associate with businesses funding criminal activity (down from 50% in 2024).

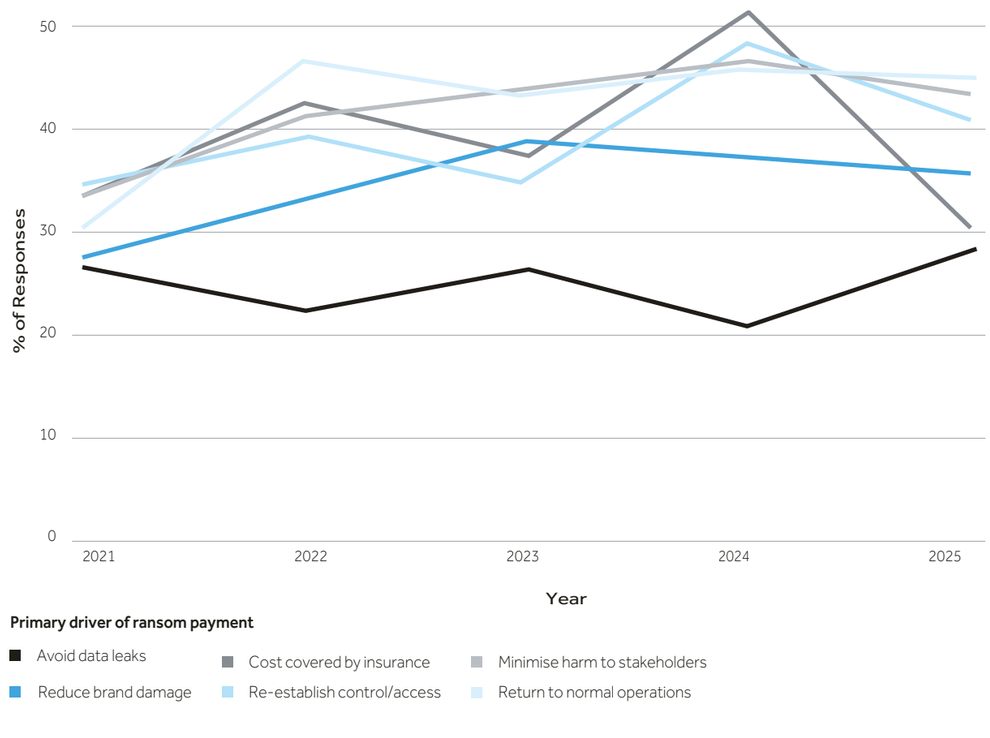
Organisations are increasingly viewing ransom payments as not just ethically problematic, but as an indication of security vulnerabilities that could affect their own operations. In terms of regulation, there is continued support for transparent reporting, with 71% of Australian business leaders still believing ransomware attacks should be mandatory to report (slightly down on 79% in 2024).

Mandatory Reporting under the Cyber Security Act 2024 (Cth) effective 30 May 2025

- 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)

5-YEAR TREND OF PRIMARY DRIVERS BEHIND RANSOM PAYMENTS

Breakdown of primary drivers from 2021 – 2025



3. Payment Scepticism

The data reveals that 81% of business leaders would still be willing to pay a ransom, however, 20% say they would pay only if there was no other choice (up from 14% in 2024). The decline in payment willingness is most pronounced among organisations with previous ransomware experience. This indicates a change in how payment is being viewed—from a primary recovery strategy to a decision of last resort.

More telling is the reduction in payment amounts. Only 18% of businesses would be willing to pay $1 million or more, down from 34% in 2024. This represents a collapse in willingness to "pay at any cost" and suggests there is growing payment scepticism throughout the business community. In other words, just because an organisation makes a ransom payment does not mean they will be able to recover all of their data or avoid being targeted again.

Organisations with incident response plans are significantly more strategic in their payment decisions. Positively, 84% of respondents now have formal plans in place compared to 80% in 2024. These plans increasingly emphasise recovery over payment, in line with evolving risk management practices.

Industry Breakdowns

Manufacturing

Prepared but still paying

68% have experienced an attack in the past 12 months, while 83% have been attacked in the past 5 years.

Executives in manufacturing organisations are more likely to have paid a cyber ransom in the past 5 years (77%), likely driven by continuity requirements. Although these organisations are more likely to pay a ransom, they are less likely to pay large amounts. The willingness to pay average amount sits at $547,000 which is significantly below the average amount that all industries are willing to pay ($906,000).

71% of manufacturing leaders say they are "very prepared" for an attack which is explained by the frequency of attacks (the highest of any industry) and the fact they are more likely to have tested their response and resilience strategies.

Financial Services

A governance and compliance advantage

Financial services organisations demonstrate a sophisticated governance approach to ransomware risk: 91% have formal board notification protocols compared to 80% of organisations overall. This maturity translates into more strategic decision-making but financial services respondents are still paying: 74% have made a ransom payment in the past 5 years. The industry's regulatory environment, particularly around anti-money laundering and terrorist financing, adds complexity.

49% consider financing criminal enterprises as a key factor in payment decisions.

Healthcare

The life-critical challenge

Healthcare shows average payment willingness in line with the overall average, but the decision-making framework is more complex due to patient safety concerns. The industry reports longer assessment timeframes and more comprehensive stakeholder notification requirements.

Restoring business operations quickly (52%) and minimising harm to stakeholders (43%) are the top payment drivers.

The need to balance systems recovery with patient safety and privacy obligations weighs heavily on boards and business leaders. When critical systems are disrupted, the duty to prioritise patient safety may justifiably take precedence.

IT & Technology

Not immune to attack

Despite presumably having the highest level of threat intelligence, detection and response capabilities, only 55% of IT and Technology organisations report feeling "very prepared" for a cyber attack. With advanced knowledge of how ransomware groups operate and greater awareness of their own vulnerabilities, IT professionals are less prone to overinflated or misguided confidence.

60% cite data security risks as a primary concern when partner businesses have paid a ransom.

Third party, counterparty and supply chain risks remain top of mind for IT and Technology professionals. Surprisingly, concerns about third party data security are significantly higher than in other industries, such as Financial Services (45%) and Healthcare (47%), where sensitive customer and patient data are often at risk.

"

Past attack experiences, while costly, can create lasting improvements. Executives must regularly test and strengthen their business resilience.

Brendan Payne, *Cyber Partner at McGrathNicol*

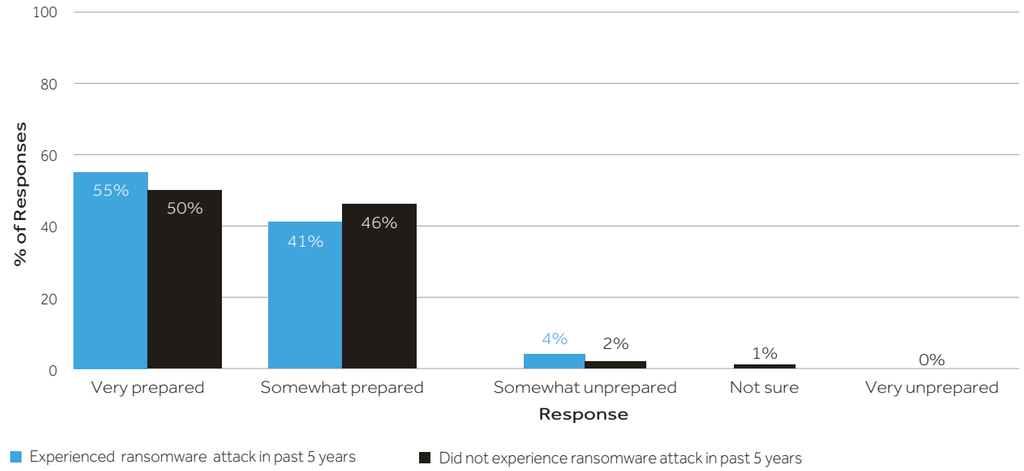
Confidence Without Complacency

The high number of business leaders who are confident in their ability to respond to a cyber attack at 96% suggests a genuine improvement in incident response capabilities but also requires careful interpretation. The breakdown shows that 53% describe themselves as "very prepared" (up from 48% in 2024) and 42% describe themselves as "somewhat prepared" (down from 45% in 2024). Further, confidence levels vary significantly by business characteristics. Executives at companies with annual revenue exceeding $10 million are more likely to say they are "very prepared" at 58%, compared to 41% of smaller businesses.

Understandably, business leaders with previous ransomware experience demonstrate greater levels of preparedness. For example, 89% of those who have experienced an attack have an incident response plan compared to 73% that haven't yet been attacked. Business leaders that have experienced an attack in the past 5 years are also more likely to support mandatory reporting (76% compared to 61%). This indicates that they understand the value of information-sharing and a more accurate assessment of the threat landscape.

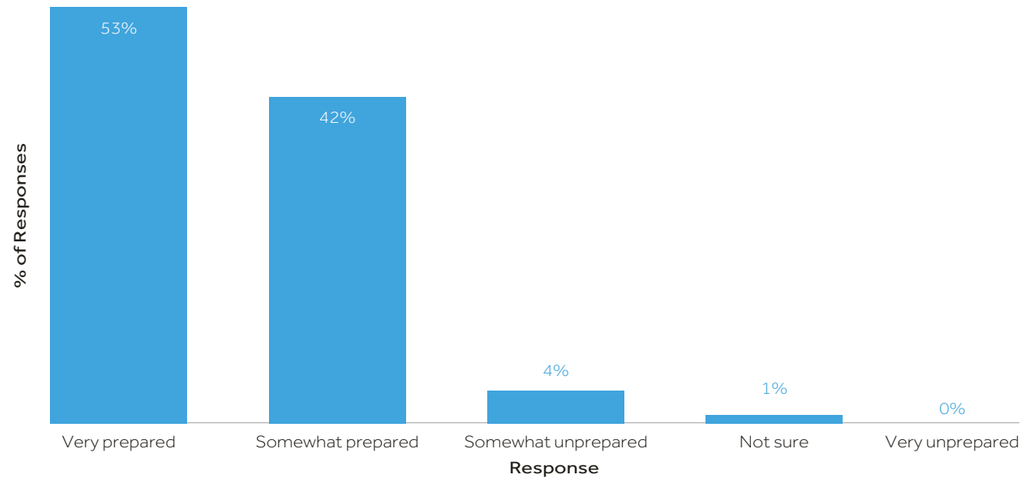
EXECUTIVE CONFIDENCE VS RANSOMWARE ATTACKS OVER THE PAST 5 YEARS

How prepared is your business in responding to a cyber attack?



EXECUTIVE CONFIDENCE OVER THE PAST 12 MONTHS

How prepared is your business in responding to a cyber attack?



Conclusion

Resilience as a Competitive Advantage

Organisations that invest in robust crisis strategies and building proactive resilience will create significant competitive advantages. The 32% of executives who believe a ransomware payment indicates that a business had inadequate safeguards in place (down from 47% in 2024) suggests that, while negative perceptions are moderating, knowledge of a cyber ransom payment remains an important factor in supplier and counterparty decisions.

The decline in willingness to pay cyber ransoms combined with growing levels of confidence signal a strategic shift away from payment-dependent recovery strategies. Higher levels of preparedness, stronger board engagement, knowledge sharing and regulatory pressure are contributing to less ransom payments. The threat remains real but organisational resilience is clearly improving.

How We Help

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 response and resilience capabilities you need to safeguard your critical business assets, people, and customers.

www.mcgrathnicol.com/our-experts/

The 2025 McGrathNicol Ransomware Survey was conducted online between 25 August and 3 September 2025 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 805 respondents. The findings have been weighted by business size and location, and reflect the latest ABS population estimates. As the survey reflects individual perspectives, findings should be interpreted as indicative rather than definitive of organisational behaviour.