RANSOMWARE 2025
FINANCIAL SERVICES SNAPSHOT

McGrathNicol

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. Here, we outline key findings and trends for the financial services sector.

The Governance and Compliance Advantage

Governance requirements, particularly around anti-money laundering and terrorist financing, create additional complexity for financial services leaders when responding to a cyber attack.

Financial services organisations demonstrate a sophisticated governance approach to ransomware risk, with 91% having formal board notification protocols in place compared to 80% overall. This governance maturity translates into a competitive advantage and more strategic decision-making in payment decisions. However, the sector's regulatory environment adds further complexity for leaders.

Key Findings

The threat remains real, but organisational resilience is improving

Prevalence of attacks: 69% of financial services respondents experienced a ransomware attack in the past five years, with 39% suffering a breach. This highlights the persistent threat facing the sector, despite improvements in governance and incident response. 47% of financial services respondents report experiencing an attack in the past 12 months.

Drivers for payment: 74% of respondents that suffered an attack reported paying a ransom in the past five years. This year, 39% of the financial services leaders elected to pay a ransom. The willingness to pay is influenced by the sensitive nature of financial data and the need to protect customer assets.

Regulatory pressures: Providers operate under strict governance and compliance frameworks, including anti-money laundering and terrorist financing regulations. These create tension between rapid recovery and avoiding financing criminal organisations. 49% of respondents consider criminal financing a key factor in payment decisions, and only 11% were unaware that ransom payments finance criminal activity.

Other attack types: Beyond ransomware, the top three other forms of attack experienced were phishing (45%), malware (34%), and business email compromise (34%).

Key Findings

Ransom Payments - Sector Attitudes

- 74% of financial services respondents that suffered an attack reported paying a ransom in the past five years (third highest payment rate after Transport & Logistics and Manufacturing).
- $898K – average estimated size of ransom payment.
- 42% paid within 24 to less than 48 hours with negotiation.
- Top drivers for payment include:
  - Getting back to normal business operations faster (42%)
  - Minimising potential harm to stakeholders (37%)
  - Reestablishing control and access to critical infrastructure and systems (42%)
- 93% say knowledge of a ransomware payment from a business in the supply chain would negatively impact their perception of that business.

Preparedness and Resilience

- 47% believe their business is very prepared to respond to a cyber attack.
- 87% have an incident response plan for a cyber attack.
- Average time taken to assess and report an attack to stakeholders was 20.12 hours.
- 98% are insured against ransomware, with average coverage of $1.31 million.

What We Are Seeing

Ransomware remains a dynamic and significant risk for financial services with APRA and ASIC both reinforcing the need for genuine cyber resilience, beyond just compliance.

Recent attacks in the superannuation industry have exposed vulnerabilities in credential management and authentication, prompting APRA to mandate sector-wide adoption of multi-factor authentication (MFA) by August 2025. The superannuation sector's experience highlights how basic security gaps, such as non-enforced MFA and weak password practices, can lead to large-scale credential stuffing and fraud, even when core systems are mature.

Banking, while highly advanced in its cyber posture, faces persistent risks from its extensive supply chain. Recent breaches have shown that third-party vendors and interconnected platforms can be exploited to bypass otherwise robust controls, making continuous monitoring and zero trust approaches essential. APRA's latest cyber resilience assessments reveal that many financial institutions still lack rigorous third-party risk management and regular testing of incident response plans, increasing exposure to cascading impacts from supply chain attacks.

Across the sector, opt-out or unenforced security controls, especially for MFA, are no longer acceptable. APRA and ASIC expect mandatory, phishing-resistant MFA for all critical systems and customer-facing portals, with regular reviews to ensure coverage and effectiveness.

Institutions that fail to meet these standards risk regulatory action, reputational damage, and financial loss. By prioritising enforced security, robust supply chain oversight, and continuous improvement, financial services organisations can better protect customer assets, maintain trust, and meet rising regulatory expectations.

> "The lesson from recent breaches is clear: security must be enforced by default, not left to user discretion."
>
> **Darren Hopkins,** *Head of Cyber*

Actions to Take Now

Tactical Recommendations

- Patch edge devices fast. The prevalence of Zero Day issues demands active patching regimes.
- Assume breaches until proven otherwise.
- Implement identity-centric zero trust.
- Maintain best-practice IT hygiene; retire or isolate legacy technologies and actively look to manage aged and legacy platforms.
- Achieve full stack visibility: log everything, analyse quickly.
- Test your incident response plan under realistic stress.
- Integrate geopolitical intelligence into Cyber Threat Intelligence capability.

Strategic Recommendations

- Exercise the Board in cyber crisis roles.
- Map and continuously assess supply chain dependencies.
- Build a security-first culture and consistently upskill employees.
- Adopt robust data governance frameworks.
- Harmonise incident playbooks with regulatory expectations and AU disclosure rules.

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 now an always-on 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.

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.

Contact Us

Get in touch to learn more about financial services cyber attack trends and best practice strategies that the most resilient organisations are putting in place now.

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

Mark Wroniak
Financial Services Co-Lead
+61 2 9338 2670
mwroniak@mcgrathnicol.com

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.

McGrathNicol

For more information visit
mcgrathnicol.com