RANSOMWARE 2025
HEALTHCARE 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 healthcare sector.

The Life-Critical Challenge

Healthcare, pharmaceutical and aged care providers face urgent and complex decisions when confronted by ransomware attacks. When critical systems are disrupted, the duty to preserve patient and client safety and resident wellbeing may justifiably take precedence. Leaders must navigate these pressures with care, transparency, and resilience.

While 50% of sector respondents report feeling "very prepared" for a cyber attack, the reality is nuanced. Decision-making frameworks in health and aged care are shaped by patient and client safety, privacy obligations, and the need for comprehensive stakeholder engagement. Boards and executives must weigh the risks of data exposure against the imperative to restore essential services for vulnerable patients and residents.

Key Findings

Threats and Resilience

Prevalence of attacks: 57% of healthcare respondents experienced a ransomware attack in the past five years, with 36% suffering a breach. This underscores the persistent threat facing the sector, despite growing resilience.

Drivers for payment: The top two drivers for payment decisions across the sector were restoring normal business operations quickly (52%) and minimising harm to stakeholders (43%), highlighting the sector's focus on safety. Not having sensitive information leaked on the dark web was cited by 24%.

Regulatory pressures: Providers operate under strict privacy and safety regulations, including Quality Standards frameworks, professional and product regulatory oversight, clinical accreditation standards, and the Privacy Act. These frameworks can create tension between the need for rapid recovery and the imperative to protect sensitive information.

Other attack types: Beyond ransomware, the top three other forms of attack experienced were phishing (37%), malware (30%), and exploiting unpatched vulnerabilities (29%).

Key Findings

Ransom Payments - Sector Attitudes

- The willingness to pay a ransom is in line with the overall respondent average, but the decision is more complex due to patient safety considerations.
- 43% paid within 24 to less than 48 hours with negotiation.
- Top drivers for payment include:
  - Restoring normal business operations quickly (52%)
  - Minimising harm to stakeholders, including patients and residents (43%)
  - Reducing brand damage with stakeholders and the public (40%)
- 87% of respondents say that knowledge of a ransomware payment from a business in their supply chain, or a business they were associated with, would impact their perception of that business.

Preparedness and Resilience

- 50% believe their business is very prepared to respond to a cyber attack.
- 73% say their business has an incident response plan, and 94% say the board would be notified in the event of an attack.
- Average time taken to assess and report an attack to stakeholders was 15.10 hours.
- 85% are insured against ransomware, with an average coverage amount of $1.11 million.

What We Are Seeing

The sector continues to face persistent and evolving ransomware threats, with attackers increasingly targeting life-critical systems and sensitive personal data.

Recent incidents have disrupted hospital operations, delayed patient care, and forced organisations to revert to manual processes, highlighting the sector's vulnerability to cyber disruption.

Regulators such as the Office of the Australian Information Commissioner (OAIC) and the Australian Cyber Security Centre (ACSC) have responded with heightened scrutiny and sector-specific guidance. The OAIC reports that the healthcare sector receives the largest proportion of notifications under the NDB scheme, with malicious or criminal cyber incidents (including ransomware attacks and compromised or stolen credentials) among the commonly cited causes. These agencies emphasise the need for robust privacy, security, and breach notification practices, as well as proactive investment in modern security controls and regular crisis simulations.

Our work across the sector shows that organisations with strong, regularly tested incident response plans and a culture of cyber awareness are better able to recover and protect those in their care. However, the sector's reliance on legacy systems, increased adoption of electronic health records, the large diverse workforce and third-party vendors continues to create vulnerabilities.

Transparent communication, ongoing staff training, and comprehensive third-party risk management are essential for building resilience and maintaining trust.

> "Organisations with strong, regularly tested incident response plans and a culture of cyber awareness are better able to recover and protect those in their care."
>
> **Darren Hopkins,** *Head of Cyber*

Actions to Take Now

There are varying degrees of cyber maturity levels across the sector. Larger providers are often more advanced but exposed to vulnerabilities inadvertently created by less mature suppliers and partners.

Tactical Recommendations

- Patch medical and aged care devices promptly.
- Assume breaches until proven otherwise.
- Implement identity-centric zero trust (strong MFA (Multi-Factor Authentication) and continuous monitoring).
- Maintain best-practice IT hygiene, retiring or isolating legacy technologies and systems.
- Achieve full stack visibility: log everything, analyse quickly.
- Test incident response plans with realistic scenarios, including patient care disruptions and resident safety risks.
- Integrate geopolitical intelligence into OT (Operational Technology) alerting.

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 to recognise emerging threats.
- Adopt robust data governance frameworks.
- Harmonise incident playbooks with disclosure rules.
- Manage the emerging threat that AI poses to operations, as organisations look to implement new technologies.
- Budget to invest in increased cyber resilience to match increased investment in digital technology.

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 health and aged care 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

Selina Gerner
Health & Aged Care Co-Lead
+61 7 3333 9848
sgerner@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