Healthcare in the crosshairs: Cyber threats and how to stay safe

August 2025

Fujitsu Cyber

FUJITSU

Fujitsu-Public

Executive summary

The healthcare industry in Australia and New Zealand (ANZ) has increasingly become a prime target for cyber-attacks, driven by the high value of medical data and the operational vulnerability of healthcare systems. Last year, Australia ranked 11th globally for breached accounts, with over 47 million accounts compromised [1], a 12x increase from the previous year.

Motivations

Cybercriminals are drawn to the healthcare sector for several reasons. Cyberattacks can cause instrumental operational disruption to hospital systems and jeopardise critical procedures and patient care. The most concerning factor is that real patient lives are at stake, creating immense urgency during an attack and giving cybercriminals considerable leverage to demand high ransoms. The potential for harm goes far beyond financial loss and directly impacts human health and safety.

Another notable motivation is the high value and sensitivity of medical data. Healthcare records are significantly more valuable on the dark web than other types of personal data [2], as they contain personal health information (PHI), financial details, and medical histories. This combination makes this data ideal for identity theft and fraud.

This report highlights:

- The evolving threat landscape targeting digital health.
- Case studies of recent cyber incidents impacting ANZ healthcare.
- Common attacker tactics and strategic recommendations for defence.

The current state of cyber in healthcare

Healthcare remains one of the most targeted industries for cybercriminals. Both healthcare and finance have emerged as the two hardest-hit sectors by cyberattacks in Australia [3]. Recent attacks in the ANZ region include:

MediSecure suffered a high-profile ransomware attack in 2024, compromising sensitive eScript infrastructure [4].

Adelaide Women's Health Clinic [5] confirmed a Termite ransomware attack [6], raising concerns over patient confidentiality.

St Vincent's Health Australia experienced a serious cyber incident in December 2023, impacting hospitals across VIC and NSW [7].

Synnovis (UK), a diagnostic provider, suffered a cyberattack that was cited as a contributing factor in a patient's death [8], illustrating the real-world risks of healthcare cyber breaches.

Key statistics

9%

9% of all interactive intrusions globally target the healthcare sector, according to CrowdStrike [9].

47m

Australia saw 47 million breached accounts in 2024 [1], a 12x increase from the year prior.

Outdated medical systems and unsupported software, including legacy Windows servers, old imaging systems remain as widespread vulnerabilities.

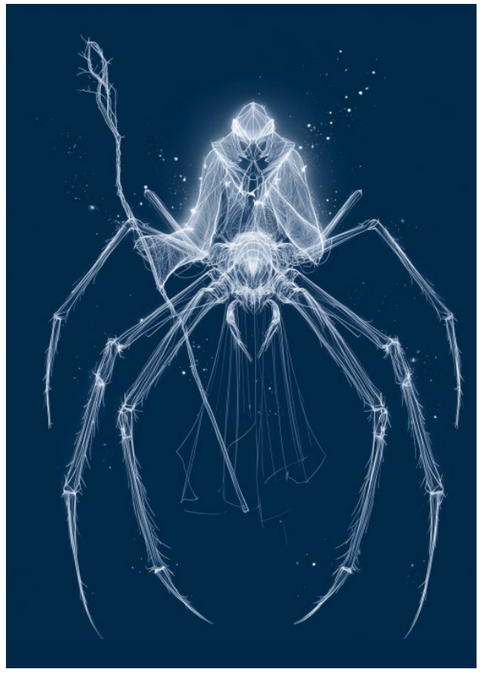
The sensitivity of the data stored within healthcare systems, including personal health information (PHI), financial records, and sensitive research data, makes this sector particularly attractive to cybercriminals. The implications of these attacks are severe, affecting not only the financial stability of healthcare organisations but also patient safety and trust.

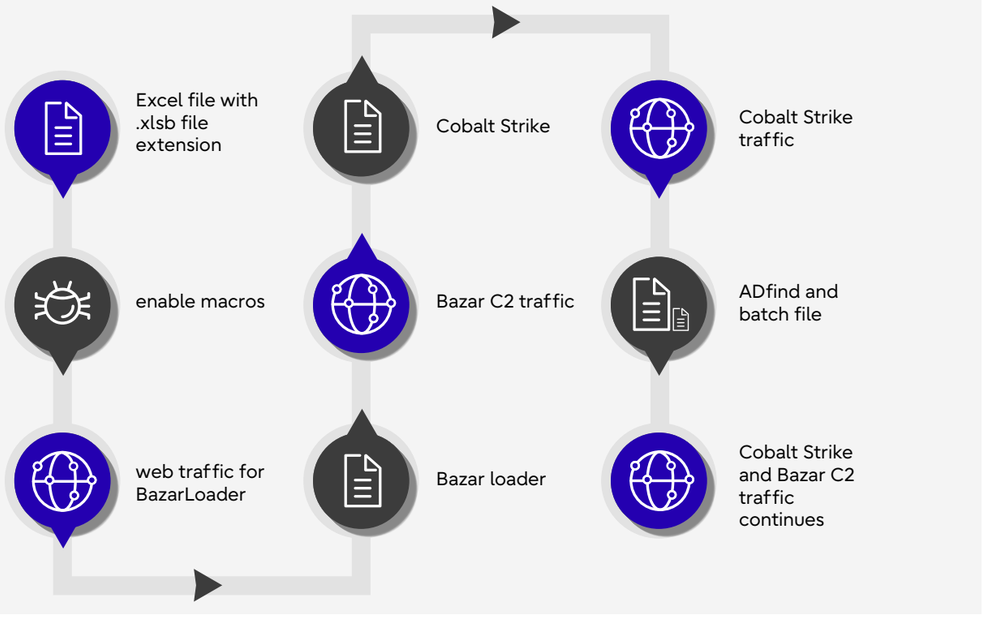
Case study: 1

Ransomware

Ransomware has proven to be a significant risk that the healthcare industry faces.

These attacks can have devastating consequences, including the potential for loss of life. A tragic example is the attack on Synnovis [10], a British diagnostic service provider, where the cyber-attack was cited as a contributing factor in a patient's death [11]. This incident emphasises the critical nature of cybersecurity in healthcare, where timely access to medical data can be a matter of life and death.





Many ransomware incidents initiate through some form of social engineering (Case Study 2). But focusing purely on the initial access vector from the point of a defender can prove inefficient. Instead, adopting a defence in depth [12] approach is essential for healthcare organisations to enhance their security posture and mitigate risks effectively.

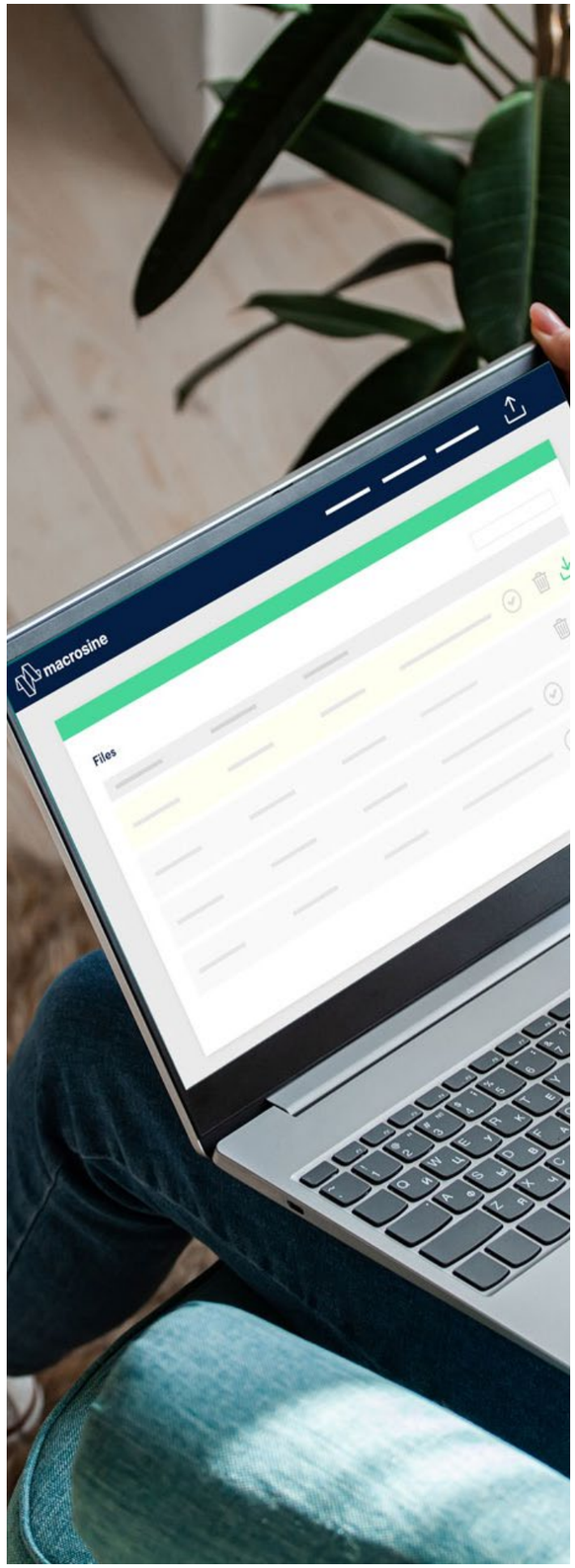
One of the most prolific groups targeting the healthcare sector in the early 2020s was WIZARD SPIDER [13]. They were attributed to the attack on the Irish Health Service Executive [14], which demonstrated the potential impact such attacks can have. Analysing the attack chain employed by WIZARD SPIDER provides valuable insights into how healthcare organisations can bolster their defences.

The attack chain of WIZARD SPIDER typically begins with the user being deceived into executing loader malware, often delivered through a malicious Microsoft Office document with macros enabled. Once executed, the malware employs living-off-the-land techniques, utilising legitimate system tools such as regsvr32.exe to establish communication with the command-and-control (C2) network. This loader is also responsible for fetching and executing subsequent stages of the malware, leading to further compromise of the system.

Given the reliance on Microsoft Office macros in the attack chain, an effective mitigation strategy is to implement the Australian Cyber Security Centre's (ACSC) Essential Eight framework, specifically the recommendation to "Restrict Microsoft Office macros." This measure significantly reduces the risk of initial compromise by preventing unauthorised execution of potentially malicious macros.

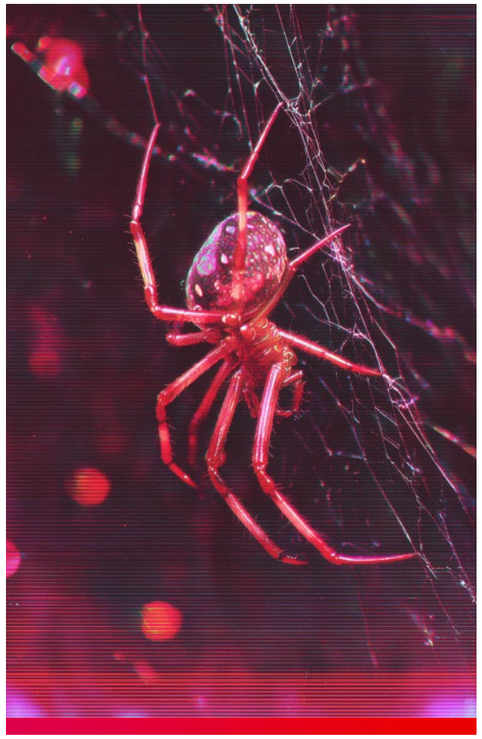
To maintain the productivity of Office macros while keeping secure, learn more about our Macrosine tool here >

macrosine®



Case study: 2

Social engineering - SCATTERED SPIDER



A notable trend in recent cyber threats is the increased use of social engineering techniques.

Criminal groups, such as SCATTERED SPIDER [15], have gained notoriety for their sophisticated methods of manipulation. This group is financially motivated and has been linked to high-profile attacks, including the cyber-attack on Qantas [16].

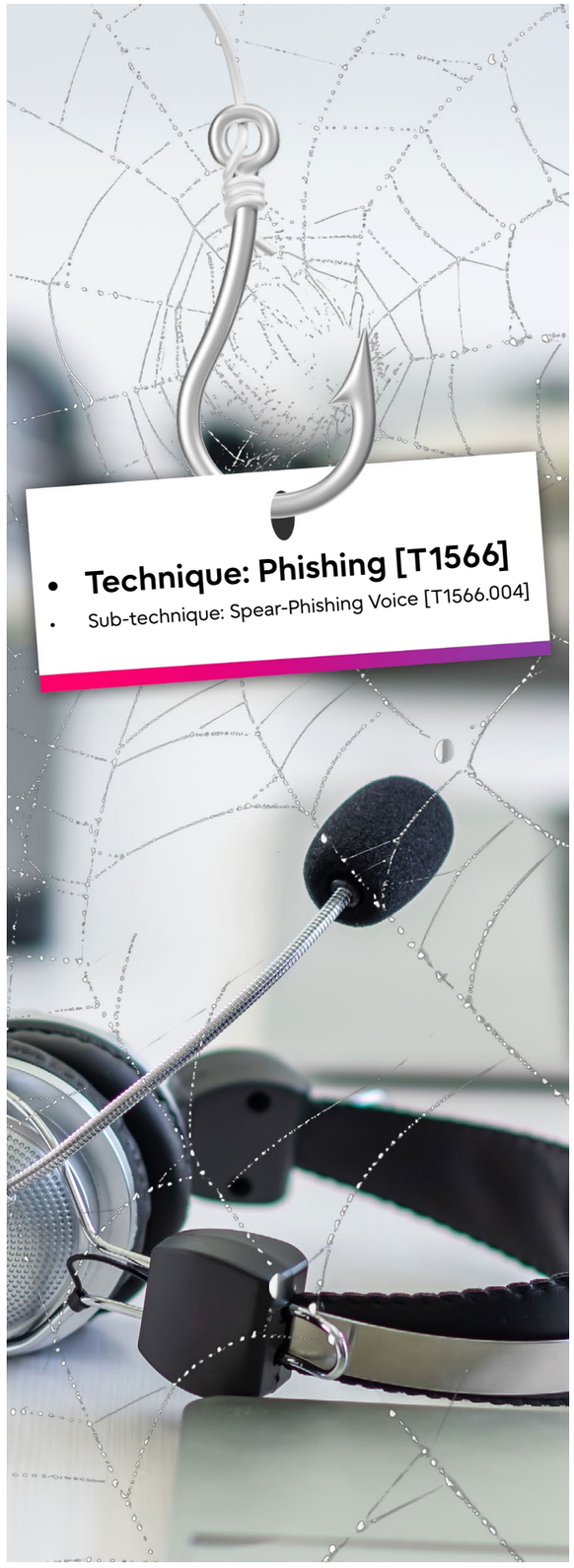
While SCATTERED SPIDER has not primarily targeted the healthcare industry, their sector-by-sector approach raises concerns about potential future attacks on this critical sector.

SCATTERED SPIDER has demonstrated a strategic targeting pattern, moving through various industries in a similar order:

Given this trend, it is crucial for healthcare organisations to familiarise themselves with the tactics employed by this group to prepare for a possible pivot to healthcare in the future. The techniques utilised by SCATTERED SPIDER are not exclusive to this group; they reflect common strategies employed by numerous attackers to gain initial access to environments.

A specific example of how this group is utilising phishing is the use of phone calls to users, posing as employees of the internal help desk. They may then direct the user to a website that installs some form of Remote Monitoring and Management (RMM) tool. This then allows the group to establish a connection to the host. From there the group can perform a variety of tactics to perform privilege escalation and lateral movement.

This group will conduct in depth OSINT (Open-Source Intelligence), through mediums like employee's social media, company social media accounts and anything they can find that would be of use.



Case study: 3

Nation state attacks

Dynamite Panda has been involved in targeted intrusions dating back as far as 2009.

They have been known to target critical infrastructure including healthcare providers, pharmaceutical companies and biotechnology firms. In 2014, Dynamite Panda compromised a large hospital operator in the US, Community Health Systems, and was responsible for the theft of 4.5 million patient records.

With sophisticated and highly targeted attacks, Dynamite Panda's tradecraft is marked by a wide range of exploit based initial access techniques. The group is known to develop custom exploits, incorporating recently discovered vulnerabilities as well as their own zero-day vulnerabilities. Initial access often occurs through internet browsing vectors such as browser hijackers and vulnerabilities in browser plugins and libraries.

Although there have been efforts to improve security, the medical industry often has a bigger reliance on legacy and vulnerable systems compared to other industries. Strict regulations and limited funding make it difficult to retire or upgrade these systems, creating an attractive target for advanced persistent threats (APTs).

Focusing solely on mitigating the initial access phase of an attack is not sufficient. To effectively reduce risk, organisations must also disrupt attacker progression across the entire attack chain. By prioritising higher maturity levels of frameworks such as the Essential Eight, organisations can implement more robust security controls that significantly lower both the likelihood and impact of a successful intrusion. Key areas of focus should include:

- **Restricting the scope of system and application access**
- **Utilising Just-in-Time administration**
- **Analysing event logs for servers and workstations**
- **Restricting unnecessary executions through application control**
- **Implementing network segmentation**

Utilising these post-compromise controls on top of initial-access protection such as EDR can contain intrusions more effectively even when dealing with sophisticated attackers.

Common attacker tactics and strategic recommendations for defence

Threat intelligence briefing

A July 2025 threat intelligence briefing revealed evolving tactics by cyber adversaries, many of which pose a direct threat to healthcare organisations due to their reliance on cloud services and high-stakes operational environments.

Social engineering surge

As technical defences improve, attackers increasingly exploit human vulnerabilities. Vishing (voice phishing) and IT help desk impersonation are on the rise, with adversaries requesting password or MFA resets to gain access to single sign-on (SSO) systems and cloud applications.

Generative AI

AI is lowering the barrier for cybercrime. Adversaries now use generative AI to create fake LinkedIn profiles, deepfake videos and voice clones for Business Email Compromise (BEC), and realistic phishing content that distributes malware at scale.

Cloud and SaaS exploitation

Threat actors are now “cloud-conscious”, targeting the cloud control plane and SaaS environments. Evolved password spraying attacks, stolen SSO credentials, and unsecured cloud databases enable widespread compromise and downstream attacks.

Targeting network devices

Perimeter devices remain prime targets due to persistent security gaps. Adversaries chain exploits and abuse built-in features for remote code execution, often leveraging public vulnerability research to enhance their methods.

Key defensive priorities emphasised by the briefing:

1. Secure identities
2. Defend the cloud
3. Eliminate cross domain visibility gaps
4. Adversary-driven patching
5. Know your adversary

How healthcare in ANZ can stay ahead of cyber threats

To mitigate the growing cyber risk facing the healthcare sector in Australia and New Zealand, organisations must move beyond reactive security postures and adopt a proactive, layered cyber defence strategy. Based on observed attacker tactics and known vulnerabilities across healthcare networks, the following recommendations are critical:

Adopt the ACSC Essential Eight (E8)

In Australia, apply the Essential Eight mitigation strategies to build baseline cyber hygiene, including focusing on application control, patching, MFA, and restricting admin privileges.

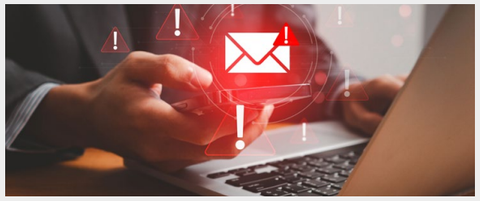
Implement defence-in-depth

Deploy a layered security approach including:

- Email filtering and anti-phishing controls
- Endpoint Detection and Response (EDR)
- Strong identity access controls with MFA
- Centralised logging and continuous monitoring
- Regular vulnerability assessments and penetration testing

Build cyber resilience

- Develop and test an Incident Response Plan (IRP)
- Maintain business continuity and disaster recovery plans
- Consider cyber insurance as part of broader risk management



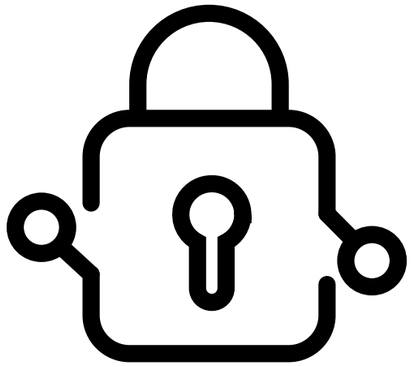
Strengthen human defences

Run regular, role-specific cybersecurity awareness training and phishing simulations to reduce the risk of social engineering and human error.

Why Fujitsu cyber?

As a trusted cybersecurity partner across Australia and New Zealand, Fujitsu Cyber brings deep expertise in defending the healthcare sector against complex and evolving threats. We offer a full spectrum of services to support your organisation's cyber resilience journey.

Our capabilities include:



Stay compliant, remain protected

www.fujitsu.com/au/services/security

Managed Security and Security Operations Centre (SOC) Services

Real-time threat detection, EDR, security event monitoring, and incident response, delivered by our 24/7 Security Operations Centre and backed by actionable threat intelligence.

Digital Forensics and Incident Response (DFIR)

Expert-led support for incident investigations, incident response planning, and readiness, including tabletops and crisis simulations, to ensure rapid containment, eradication, recovery, and resilience in healthcare environments.

Governance, Risk and Compliance (GRC)

Assistance with industry frameworks (e.g. ISO 27001, ACSC Essential Eight, ISM, etc.) to ensure regulatory compliance and security maturity.

Penetration Testing and Red/ Blue Teaming

Real-world attack simulations, including web apps, infrastructure, and social engineering assessments to identify exploitable weaknesses before adversaries do.

Healthcare-specific cyber strategy

We understand the operational sensitivity of clinical environments and build security strategies that preserve system uptime, patient care, and regulatory obligations. Whether you're seeking to uplift your baseline security, respond to a recent incident, or design long-term resilience into your digital health infrastructure, Fujitsu Cyber is your strategic trusted security partner.

This article was created by:

Thomas Hacker
Cyber Security and Threat Intelligence Analyst
Fujitsu Cyber

Hilary Bea
Senior Consultant
Fujitsu Cyber

Ed Goodacre
Digital Content Specialist
Fujitsu Cyber

References

[1] Surfshark, "Data breach recap 2024," Surfshark Research, [Online]. Available: https://surfshark.com/research/study/data-breach-recap-2024?srsltid=AfmBOorbnvlkWnERScYUxCYx94XKINJiHkLipldRdpDczv4lH5POHI_O. [Accessed: 31-Jul-2025].

[2] F. Ramirez, "The Dark Web & Healthcare: Why Your PHI is a Prime Target," HIPAA Vault, 26-Mar-2025. [Online]. Available: https://www.hipaavault.com/resources/dark-web-healthcare-phi/. [Accessed: 31-Jul-2025].

[3] Cyble, "Cyberattacks are costing Australia's key industries," Cyble, 08-Jul-2025. [Online]. Available: https://cyble.com/knowledge-hub/cyberattacks-are-costing-australias-key/. [Accessed: 31-Jul-2025].

[4] R. Bristow, "Medisecure data breach: Cyber hack affects 12 million people," ABC News, 18-Jul-2024. [Online]. Available: https://www.abc.net.au/news/2024-07-18/medisecure-data-cyber-hack-12-million/104112736. [Accessed: 31-Jul-2025].

[5] CyberDaily, "Exclusive: Adelaide Women's Health Clinic confirms cyber attack," CyberDaily, [Online]. Available: https://www.cyberdaily.au/security/12326-exclusive-adelaide-womens-health-clinic-confirms-cyber-attack. [Accessed: 31-Jul-2025].

[6] Splunk, "Termite ransomware analysis," Splunk, [Online]. Available: https://www.splunk.com/en_us/blog/security/termite-ransomware-analysis.html. [Accessed: 31-Jul-2025].

[7] S. Macdonald, "Questions deepen over St Vincent's, Victorian courts hacks," The Sydney Morning Herald, 12-Jan-2024. [Online]. Available: https://www.smh.com.au/technology/questions-deepen-over-st-vincent-s-victorian-courts-hacks-20240112-p5ewrd.html. [Accessed: 31-Jul-2025].

[8] Digital Health, "Patient dies as a result of cyber attack on NHS pathology provider," Digital Health, 06-Jun-2025. [Online]. Available: https://www.digitalhealth.net/2025/06/patient-dies-as-a-result-of-cyber-attack-on-nhs-pathology-provider/. [Accessed: 31-Jul-2025].

[9] CrowdStrike, 2025 Global Threat Report, [Online]. Available: https://go.crowdstrike.com/2025-global-threat-report.html. [Accessed: 31-Jul-2025].

[10] NHS England, "Synnovis cyber incident – public questions and answers," 15 October 2024. [Online]. Available: https://www.england.nhs.uk/synnovis-cyber-incident/questions-and-answers/.

[11] S. Alder, "Patient Death Linked to Ransomware Attack on Pathology Services Provider," 27 June 2025. [Online]. Available: https://www.hipaajournal.com/patient-death-linked-to-ransomware-attack/.

[12] Fortinet, "What Is Defense In Depth?," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/defense-in-depth#:~:text=Defense%20in%20depth%20is%20a%20strategy%20that%20leverages,ensure%20that%20threats%20are%20stopped%20along%20the%20way.

[13] Wikipedia, "Wizard Spider," [Online]. Available: https://en.wikipedia.org/wiki/Wizard_Spider.

[14] S. Gatlan, "HHS: Conti ransomware encrypted 80% of Ireland's HSE IT systems," 4 Febuary 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/hhs-conti-ransomware-encrypted-80-percent-of-irelands-hse-it-systems/.

[15] Wikipedia, "Scattered Spider," [Online]. Available: https://en.wikipedia.org/wiki/Scattered_Spider.

[16] Qantas, "QANTAS CYBER INCIDENT," 2 July 2025. [Online]. Available: https://www.qantasnewsroom.com.au/media-releases/qantas-cyber-incident/.

Fujitsu Cyber

www.fujitsu.com/au/services/security