Australia's Horizon Cyber Security Initiative: What it Means for Industry

David Gaul
University of Queensland

Executive Summary

Every 3.2 seconds, another company falls victim to ransomware attacks; these incur an average of 23 days downtime. With the prolific onset of AI-enabled ransomware attacks reducing threat actor's lateral movement time from 8 hours to 22 seconds, traditional technology-driven cyber security methods are failing. To keep pace against modern-day threats, the cyber security industry needs to adapt with it, developing cutting-edge technology, educated individuals and robust governance frameworks.

In this article, we use the Australian Government as a case study for effective, forward-moving mitigation to rising cyber threats. Australia, which is a top-10 global cyber power despite its small population size, sets a strong example for effective cyber governance and resilience. Here, we analyse their cyber security foundation and its implications for the future of threat actors and the nation's cyber strength. Finally, we distil these findings into actionable insights and what they mean for cyber security professionals in industry.

1 Introduction - The Ransomware Threat

In March 2026, German political party "Die Linke" was hit by one of the largest ransomware attacks of the year. Qilin, a Russian-speaking ransomware gang, made Die Linke the third German political party to have been targeted by cyber attacks.

This particular incident is a symptom of a catastrophic issue; cyber extortion has mutated into an intricate business model. Mature ransomware gangs have adopted ransomware-as-a-service (RaaS) structures, incorporating HR departments, help desks, negotiators and affiliate structures in a twisted mirror of legal corporations. Alongside this switch in structuring, major strains have evolved from simple extortion to prioritise societal disruption, espionage and state-aligned hybrid warfare. Qilin's attack against Die Linke highlights the tendency for ransomware gangs to act as proxies of geopolitical hybrid warfare. In this regard, it's reminiscent of the NotPetya virus: a "Weapon of Mass Destruction" intended primarily to destabilise Ukrainian infrastructure.

The propensity for ransomware gangs to elicit large-scale cyber disruptions is further propagated through the adoption of new technologies. Google's Mandiant M-Trends Report highlighted that AI has reduced malware breakout time to 22 seconds, whereas human-driven methodologies require 8 hours. This represents the median time taken for adversaries to hand off access or move laterally across a network after breaching the perimeter. Under these conditions, traditional methods of detection, triage and incident response become obsolete; if organisations rely solely on humans to detect and contain a cyber threat, they've already lost.

Ransomware Attack Metrics

- **3.2 Seconds:** The projected frequency in which ransomware attacks claim another victim.
- **22 Seconds:** The median breakout time for modern ransomware to execute lateral network movement.
- **23 Days:** The average network downtime of businesses per ransomware attack
- **$25 Billion per Year:** The estimated annual cost to Australia by aggregate cyber incidents.
- **$35 Billion:** The projected economic damage resulting from a single catastrophic cyber security incident.
- **50% Increase:** The year-on-year growth in the average self-reported cost of an individual cybercrime reported by Australian businesses.
- **60% of Breaches:** The proportion of recorded security breaches caused by human error.

By 2026, the spread of AI-facilitated cyber crime has progressed to catastrophic proportions. Malicious actors systematically deploy automated exploitation pipelines, exceeding human-speed triage and accelerating operation tempo. Data breaches are increasingly reporting attacker-driven artificial intelligence. Furthermore, exploitation of vulnerabilities in edge devices (i.e. modems, routers, VPNs) has risen from from 3% in 2023 to 22% in 2024. The ransomware attack statistics derived in info-box 1 show that traditional, reactive methods of incident response commonly employed in industry have become obsolete within the modern threat environment. Outdated methodologies guarantee compromise, which can have devastating effects before human-driven isolation protocols can even begin.

2 Horizon - Redefining Cyber Resilience

Because traditional, reactive defence postures break against this new reality, a new global benchmark is required. Australia, which has been identified by Harvard Kennedy Business School as a top-10 global cyber power despite its small population size of 27 million, sets a strong example for developing cyber resilience strategies. Within this report, we use Australia and their emerging cyber security infrastructure as a case study and reference point for future nation-level cyber initiatives, and discuss its implications for the cyber security industry in Australia. By 2026, they are beginning stage 2 of their "Horizon" movement; a three-stage framework serving as a leading benchmark for global improvement in cyber security posture.

Horizon, which was which first commenced in 2023, delineates a three-stage architectural model to achieve global operational primacy by 2030 which is outlined in Figure 1. While the first stage, Horizon 1 (2023-2025), focused primarily on foundational cyber capabilities, Horizon 2 executes the systematic expansion of cyber maturity across the broader macroeconomic landscape, producing a tested governance architecture applicable for international standardisation. This is executed through 6 "Shields" - defence initiatives to bolster Australia's cyber resilience and robustness (Figure 2).

Among these shields, 2 major themes merge; bolstering the people, processes and technologies underpinning Australia's cyber resilience before taking the fight back to threat actors.

2.1 Human Firewall

Despite the reported 22-second automated hand-off, initial delivery of ransomware strains remains surprisingly low-tech. Humans still remain the weakest link of any cyber security system. Given that 60% of cyber incidents across all sectors stem from human error (i.e. phishing), Australia is fully engaged in strengthening their "Human Firewall" through their Act Now, Stay Secure campaign. Through simple practices including password managers, multi-factor authentication, and regular

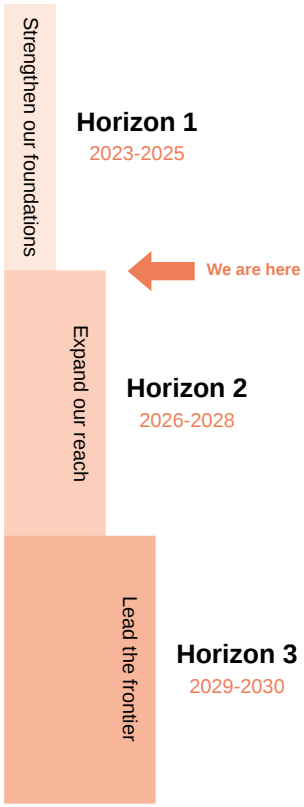

Figure 1: **Three horizons to provide review points and enable us to remain adaptive to emerging technological, economic and geo-spatial trends. Derived from: [11].**

software updates, non-technical staff are able to bypass the most common vulnerabilities exploited by threat actors. The goal of this paradigm is to cultivate a culture where people are actively looking for anomalies, transforming the workforce from the primary attack vector into the first line of active defence. Actively strengthening the human element can help contribute towards a 2.5x reduction in cyber incidents, vastly strengthening the small business sector in which 80% of cyber incidents occur.

However, generalised cyber security campaigns consistently fail to account for societal and language barriers, as well as deficiencies in technological literacy. In light of this, the Australian government has similarly invested $7 million in funding across 200 organisations to promote cyber awareness for under-represented communities. This transforms rigid technical requirements into culturally-aligned guidelines delivered through respected peer networks and local leadership. In trusting awareness delivery to established community members across Culturally and Linguistically Diverse Cohorts (CALD), seniors and people with disabilities, the Horizon program achieves scalability that traditional methods fail to

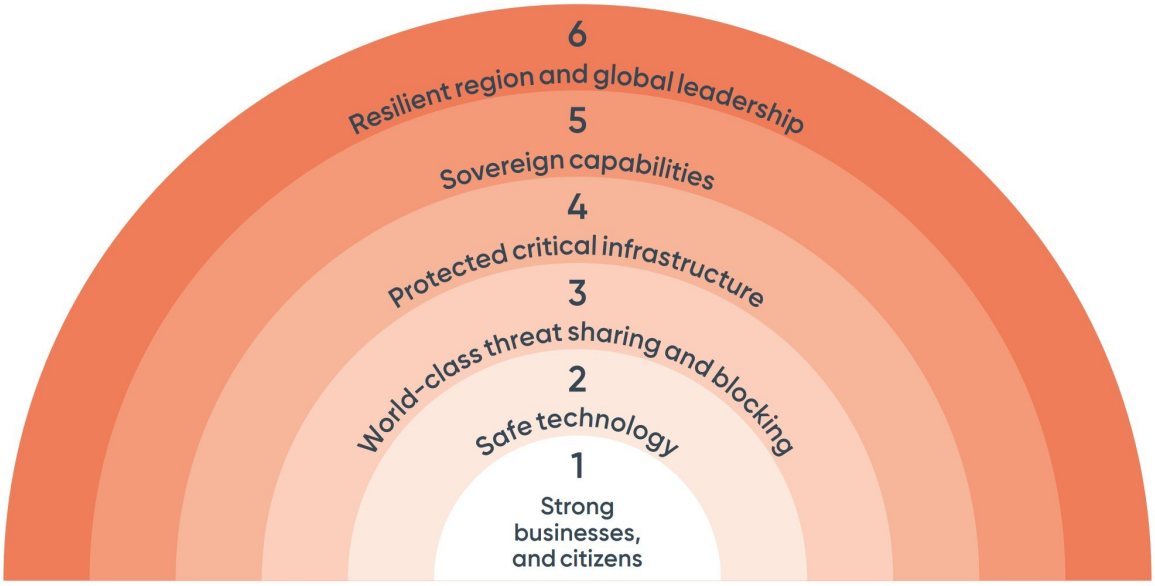

Figure 2: **Horizon's 6 shields each providing an additional layer of protection for businesses and citizens. Image sourced: [11]**

reach. By moving Horizon's impact beyond government and enterprise-level corporations, Australia is building more resilient small businesses and local communities.

Despite the increased emphasis on awareness and education, security breaches are inevitable. In these scenarios, 80% of losses are generally inflicted upon small-to-medium businesses which lack robust, enterprise-level defences. Many businesses will never recover. For this reason, the Department of Home Affairs (DHA) and ASD implemented the Cyber Health Check Tool, which equips non-specialised audience with prioritised cyber resilience road-maps. This, alongside the Small Business Cyber Resilience triage program, helps provide increased support for Australia's most critical sector.

◎ Key Finding: People-Centric Security Mitigation
Academic literature and industry reports point to an over-investment in technologies as a solution to cyber security issues. In practice, it results in an arms-race between threat actors and cyber defenders to "Build a Bigger Gun." This fails to address the elephant in the room; 60% of cyber incidents stem from human error. Investing in user awareness and education, particularly for non-technical audiences, provides a robust, scalable frontline in cyber defence which complements emerging technologies in cyber resilience.

2.2 Governance

Despite cyber security's foundation being rooted in the three pillars of people, processes and technologies, recent innovations have focused almost exclusively on technological development. Although under-regulation allows for more rapid technology development, this can come with devastating side effects. Australia's recent *Online Safety Amendment (Social Media Minimum Age) Bill 2024* is an example of utilising legislation to combat the devastating effects of social media in younger audiences. This bill represents a step in the right direction, and is planned to be followed with more effective regulation of social media and AI.

This act highlights the Australian Government's focuses on enhancing regulation of cyber security services. In a separate bid to push secure-by-design architectures, Australia's *Smart Devices Cybersecurity Labelling Scheme* is endorsing cyber-related "nutrition labels" for IoT devices and software. It gives better transparency into a product's security posture, allowing the market to promote safer and more effective solutions. In addition, mandatory ransomware payment reporting through Australia's *Cyber Security Act (2024-2025)* similarly utilises legislation to incentivise better practices. Although these shift an initial regulatory burden onto businesses, the incresed standardisation of best practices and de-incentivisation of ransomware repayments lowers the cost-benefit mechanics for RaaS models, thereby contributing to a stronger and more uniform Australian business sector. Additionally, enhanced human-centric and regulatory procedures have allowed Australia to ease the effective burden commonly resting on the

technology sector's shoulders to mitigate cyber crime.

2.3 Secure-By-Design Architecture

In spite of improvements to the people and processes behind Australia's cyber infrastructure, breaches are inevitable. With increasing rates of data theft and double extortion, securing consumer's sensitive information has become both an ethical and economic imperative. Following multiple high-profile data breaches, such as from Optus and Quantus, the Horizon initiative seeks to remedy data theft challenges through data minimisation, zero-trust architectures and post-quantum cryptography (PQC).

Under the *Digital Identity Act 2024*, Australia has transitioned its public-facing infrastructure to adopt to MyID digital identity system. Operating on zero-trust security models, this system enforces strict data minimisation. In doing so, it eliminates unnecessary duplication and transmission of sensitive personal files. Already, this has been incorporated into 15.2 million active MyID accounts across 255 government services. In November 2026, Digital ID access will be made available to industry to reduce catastrophic data breaches. In doing this, the Australian Government will help secure highly sensitive data in vulnerable industries such as real estate and healthcare.

Case Study: Optus Data Breach
Optus, Australia's second-largest telecommunications provider, suffered a crippling data breach in September 2022. This leak, which affected between 2.5-9.7 million records, gave access to sensitive consumer information including addresses, drivers licenses and passports. As a consequence, 178,000 Queensland drivers licenses were replaced and Optus suffered an estimated $1.5 billion damages to their brand.
This perfectly highlights the severity of large-scale data breaches, and highlight the push for data minimisation and PQC principles being promoted throughout the Horizon 2 initiative.

The introduction of the MyID Digital Identity system follows Australia's broader enforcement of secure-by-design architecture. The recent *Cyber Security Act 2024* and *Cyber Security (Security Standards for Smart Devices) Rules 2025* establish a mandatory security baseline for consumer smart devices entering the market. To guide enterprise adoption, the ASD published the *Foundations for Modern Defensible Architecture* in February 2025, providing a tactical baseline of design and architectural goals. Similar to the labelling scheme discussed within Section 2.2, the enhanced regulation of system architectures adds an additional regulatory overhead for businesses, but overall contributes to a more unified baseline of cyber resilience.

Although data minimisation and secure-by-design principles drastically reduce the severity of data breaches, some amount of information must always be stored on-site. Although many encryption algorithms remain robust against modern methods, quantum cryptanalysis is projected to change this within 5 years. The rising trend of "Harvest now, decrypt later" attacks has prompted ASD to formally add 2 PQC algorithms to the national cryptographic list, as well as incorporate a phase-out timeline for outdated algorithms by 2030. This synchronises with Five Eyes intelligence partners to maintain algorithmic alignment and macro-regional defensive synergy.

Aggressive data minimisation strategies fundamentally alter the mechanics of ransomware negotiations. The absence of stored, high-value data combined with robust back-ups neutralises RaaS' ability to execute single and double extortion. Shielding consumers through zero-trust data minimisation protocols directly reduces the operational liability of businesses during cyber attacks, incentivising leadership to invest in secure-by-design architectures which remain robust against modern cyber threats.

3 Taking the Fight Back to Threat Actors

Cyber security is often analogised to medieval siege warfare. In particular, defence is more difficult than attack. Modern day cyber defenders are burdened with the challenge of fortifying every vulnerability; threat actors only need to exploit one. Nowadays, the frontier of cyber defence takes inspiration from another siege warfare anecdote; offence is the greatest form of defence. By taking the fight back to threat actors, they mitigate their own vulnerabilities and transition from reactive to proactive methodologies.

This sentiment is reflected in Australia's Horizon initiative. Operation Aquila, a joint initiative between the Australian Federal Police (AFP) and the ASD, is focused on using offence as the greatest form of defence. Taking inspiration from the AN0M sting (Operation Ironside) which decimated encrypted phone systems, Australia is actively hunting threat actors to protect its people. Since its inception, it has proactively disrupted 38 threats against high-profile criminal organisations such as Lockbit and Blackcat. In doing so, the AFP and ASD are helping mitigate cyber damages and reducing critical downtime.

4 Conclusion

Traditional methods of incident response are obsolete. When ransomware attacks claim another victim every 3.2 seconds, cyber resilience has become more than building bigger walls. Through enhanced education, bolstered regulation and im-

Case Study: Operation Aquila

Operation Aquila's sanctioning capabilities are best exemplified through the case against Aleksandr Ermakov. During the 2022 intrusion against Medibank, 9.7 million health records and personally identifiable information sources were ex-filtrated. In a joint operation between the AFP and ASD, Operation Aquila enacted the inaugural deployment of its autonomous cyber sanctions legislation system. This imposed targeted financial asset freeze and travel restrictions. In criminalising transferal of financial capital to Ermakov, law enforcement have effectively neutralised his capacity to interact with cryptocurrency infrastructures and execute ransomware monetisation pipelines.

proved offensive capabilities, international alliances are actively strengthening Australia's cyber defences.

The global benchmark is evolving. In 2026, Australia officially transitioned from building foundational defences into Horizon 2: Expanding Our Reach. Cyber security is no longer an isolated IT issue, but a whole-of-society imperative. Security architects and leaders should transition from traditional, reactive cyber security implementations to raise awareness, abide by best practices and implement rigorous secure-by-design architectures. The time has passed for wishful thinking and outdated ideologies; we need to follow Australia's initiative to protect our businesses and communities.

5 credits

This study was backed by the Cybersecurity Advisor's Network's (CyAN's) global mentorship program.

David's research is funded under grant GA-192148.

Google's Notebook LM and Gemini were used in the information acquisition and drafting of this article. Final writing, proofreading and editing were performed manually

6 About the Author

With 5 years of experience in machine learning and automation, David is an aspiring cyber security analyst engaged in industry-funded R&D of cyber crime attribution techniques. His research bridges the gap between governance, legislation and technology by providing actionable insights into enhanced compliance of technology in forensic procedures. He is currently completing his PhD at the University of Queensland, with a passion for enhancing community awareness through outreach opportunities, conferences and journal articles. His areas of interest include AI, ML, legislation and ISO standards.

References

[1] AFP. AFP-led Operation Ironside smashes organised crime | Australian Federal Police. https://www.afp.gov.au/news-centre/media-release/afp-led-operation-ironside-smashes-organised-crime, June 2021.

[2] Australian Government. Online Safety Amendment (Social Media Minimum Age) Bill 2024. https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bil November 2024.

[3] Australian Government. Small Business Cyber Resilience Service. https://business.gov.au/expertise-and-advice/small-business-cyber-resilience-service, July 2025.

[4] Australian Government. What are you risking online? | Act Now. Stay Secure. https://www.actnowstaysecure.gov.au/, 2026.

[5] Australian Signals Directorate and Department of Home Affairs. Cyber Health Check Tool | Cyber.gov.au. https://www.cyber.gov.au/cyberhealthcheck, 2026.

[6] Defence Ministers. Cyber sanction in response to Medibank Private cyber attack. https://www.minister.defence.gov.au/media-releases/2024-01-23/cyber-sanction-response-medibank-private-cyber-attack, January 2024.

[7] Department of Finance. Digital ID Act 2024 | Digital ID System. https://www.digitalidsystem.gov.au/what-is-digital-id/digital-id-act-2024, 2024.

[8] Department of Home Affairs. 2023–2030 Australian Cyber Security Strategy. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy, May 2026.

[9] Department of Home Affairs. Cyber Security Act. https://www.homeaffairs.gov.au/cyber-security-subsite/Pages/cyber-security-act.aspx, February 2026.

[10] Department of Home Affairs. Horizon 1: Strengthening our foundations (2023–2025). https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/horizon-1, June 2026.

[11] DHA. Horizon 2 - Expanding our reach (2026-2028). https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/horizon-2, 2026.

[12] Google. M-Trends 2026 Report. https://cloud.google.com/security/resources/m-trends, 2026.

[13] IBM. Cost of a data breach 2025 | IBM. https://www.ibm.com/reports/data-breach, 2025.

[14] Julia Voo. National Cyber Power Index 2022 | The Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/national-cyber-power-index-2022, September 2022.

[15] Lizzie Danielson. NotPetya Malware: Analysis, Detection, Removal. https://www.huntress.com/threat-library/malware/notpetya, December 2025.

[16] NCA. International investigation disrupts the world's most harmful cyber crime group. https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group, February 2024.

[17] heise online. Qilin: Left Party reports Russian ransomware attack. https://www.heise.de/en/news/Qilin-Left-Party-reports-Russian-ransomware-attack-11227232.html, March 2026.

[18] Pierluigi Paganini. Qilin ransomware group claims the hack of German political party Die Linke, April 2026.

[19] Queensland Government. Optus data breach. https://www.qld.gov.au/community/your-home-community/cyber-security/cyber-security-for-queenslanders/case-studies/optus-data-breach, 2022.

[20] Total Assure. How Often Do Ransomware Attacks Occur in 2026: Comprehensive Frequency Analysis. https://totalassure.com/blog/how-often-do-ransomware-attacks-occur, June 2026.

[21] Verizon. 2026 Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/dbir/, 2026.

[22] Yiying Li and Rihana Whitson. Frustration mounts among Qantas customers over data breach. *ABC News*, October 2025.