NZ Incident Response Bulletin

Standard Edition –March 2026 – Issue #86

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Each Bulletin also includes a section of our own content, based on a trending theme. We'll give you a brief summary of each article, and a link to more information. Why do we publish this bulletin? Because we want to keep you up to date with the latest Forensic and Cyber Security news, so that you aren't caught by surprise – and you'll know about risks and changes before they become problems.

News:

A high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

New Zealand's Cyber Security Strategy 2026 – 2030

The Government published New Zealand's Cyber Security Strategy for 2026–2030, positioning cyber threats as a national security and economic resilience challenge and calling for a "whole of society" approach. The strategy is framed around four objectives: understand threats better, prevent and prepare, improve response, and strengthen partnerships across government, industry and communities. For executives, this signals a policy direction that is likely to influence expectations placed on organisations that deliver essential services, handle sensitive information, or underpin critical supply chains. Even without immediate new regulation, strategies typically drive agency priorities, investment, sector guidance, and (over time) stronger baseline requirements for risk management and incident reporting. Practical implications include: anticipate more cross-sector coordination during major incidents; align internal programmes to recognised frameworks; and treat resilience (business continuity, recovery, third-party risk) as equal in importance to preventative controls. Use the strategy to benchmark your roadmap and to justify investment decisions to boards and stakeholders.

New Zealand's Cyber Security Action Plan 2026 – 2027

Alongside the strategy, DPMC released an Action Plan for 2026–2027 that describes the initial steps government intends to take to turn the strategy into practical activity. While the strategy sets the long-term direction, the action plan is the near-term "delivery layer" and is therefore a useful indicator of what may change first: programme focus, guidance, coordination mechanisms, and prioritised initiatives that affect how organisations engage with government on cyber matters. For an executive audience, the action plan is relevant because it can foreshadow shifts in assurance expectations, funding, and sector engagement. It may also influence the cadence of cyber exercises and national-level preparedness activities that require participation from regulated or high-impact organisations. Review it for upcoming initiatives that could affect your operating environment, then map those to your own plans for incident readiness, supplier management, detection and response capability, and executive crisis decision-making.

Privacy Commissioner calls for significant fines and 'real consequences' for cybersecurity breaches

The Privacy Commissioner, Michael Webster, responded to the Manage My Health breach by arguing New Zealand needs stronger enforcement tools to drive better cybersecurity and privacy practices. He said current powers and penalties under the Privacy Act 2020 are not strong enough to create meaningful accountability, and pointed to larger overseas penalty regimes (including Australia) as examples of "real consequences" that change behaviour. The article notes the breach involved theft of sensitive health records and an extortion demand, which Webster said creates severe harm for individuals whose most private information could be exposed. He has launched an urgent inquiry, with interim findings expected by late April 2026, and signalled broader scrutiny of how digital service providers protect sensitive data. For executives, the message is clear: regulatory expectations are rising, and boards should treat privacy and cyber controls as core risk governance, not just IT hygiene.

Chief executives optimistic about economic recovery, fear being left behind in AI race - survey

RNZ reports on PwC's annual CEO survey, where New Zealand leaders were generally optimistic about the economy and revenue prospects, but identified technology disruption as a key concern. The cyber security angle is that NZ respondents showed comparatively weak intent to lift cyber resilience, with only about a third expecting to take significant action to improve cybersecurity in response to geopolitical risk over the next three years. That gap matters because executives are simultaneously trying to adopt AI, and AI adoption increases the attack surface through new tooling, new data flows, and staff experimentation. The article's implication for leadership teams is that cyber investment and AI enablement should move together: modernising without strengthening controls increases the likelihood and impact of incidents. This is a governance issue as much as a technical one, requiring clear ownership, measurable uplift plans, and board-level tracking of progress against priority risks.

Australia

Australians fear falling victim to AI-related crimes, deepfakes and hacks, research shows

New Australian research reported that more than half of adults are concerned about AI being used to cause harm, and nearly as many fear becoming victims of AI-enabled crime. The study's findings point to a trust and risk-management challenge for organisations deploying AI in customer-facing processes: people worry about AI being used to track location, access devices or accounts, and impersonate or deceive, with deepfake content featuring strongly in concerns. The survey also suggests widespread AI use in everyday tools (such as mapping, translation, and chatbots), and indicates a gap between perceived risk and expected likelihood of victimisation in the next 12 months. Executive implications: fraud and identity risk are becoming "brand risks" as well as security risks, and organisations should strengthen customer authentication, deepfake-resistant verification for high-risk transactions, staff awareness, and clear communications about how AI is used, what data is collected, and how misuse is detected and handled.

Cyber attack takes major chicken processor Hazeldenes offline leaving businesses without meat

A cyber incident disrupted operations at Hazeldenes, a major chicken meat processor in central Victoria, forcing the company to shut down on-site Wi-Fi and leaving parts of its production and packaging workflow unable to run normally. The operational outage quickly flowed into the supply chain, with wholesalers, pubs, butchers, and other businesses reporting shortages and needing to source product from alternative suppliers to avoid disappointing customers. Hazeldenes said it engaged cyber security investigators and is working with relevant authorities to determine what happened and restore impacted operations. The company also indicated that if any data was affected, it would notify impacted individuals as required. For executives, the key takeaway is that cyber events can cause immediate business continuity impacts even without confirmed data theft, and suppliers may become a single point of failure for downstream partners.

World

UK investigating first suspected breach of cyber sanctions

UK authorities have opened their first investigation into a suspected breach of the country's cyber sanctions regime, signalling that enforcement is moving from policy to practice. HM Treasury confirmed that the Office of Financial Sanctions Implementation (OFSI) has logged up to five potential breaches, all linked to firms in the financial services sector, but declined to provide case details to avoid prejudicing investigations. The development follows years in which OFSI reported no detected cyber-sanctions breaches, raising questions about visibility and monitoring effectiveness. The article notes that OFSI has recently expanded its capabilities, including increased staffing, advanced analytics, specialist datasets, and cryptocurrency investigation tools, reflecting the complexity of cyber-related payment chains and cross-border intermediaries. While no enforcement actions have yet been completed, the potential consequences are significant: civil penalties can reach £1 million or 50% of breach value, criminal fines can be unlimited, and senior managers may face up to seven years in prison.

ASIC action sees FIIG Securities ordered to pay $2.5 million over cyber security failures

Australia's corporate regulator, ASIC, has secured Federal Court orders requiring FIIG Securities Limited to pay $2.5 million in civil penalties, plus $500,000 towards ASIC's costs, after the firm admitted prolonged cyber security failures. ASIC says FIIG's inadequate controls over more than four years contributed to the impact of a 2023 cyber-attack in which about 385GB of confidential information was stolen and some highly sensitive customer data was later leaked on the dark web. FIIG notified around 18,000 clients that personal information may have been compromised, including identity documents and financial identifiers. The court also ordered FIIG to implement a compliance programme and engage an independent expert to uplift cyber security and cyber resilience. ASIC framed the outcome as a regulatory marker, emphasising that cyber resilience is now a licence-to-operate expectation for financial services firms, and that weak governance, resourcing, monitoring, and basic hygiene controls can lead to enforcement action.

Attackers Now Need Just 29 Minutes to Own a Network

Industry reporting citing recent threat intelligence suggests attackers can move from initial access to lateral movement in roughly 29 minutes on average, shrinking the window defenders have to stop a breach from spreading. The speed-up is linked to heavy use of stolen credentials and "living off the land" activity that looks like normal admin behaviour, alongside more automated, repeatable attack playbooks. Unmanaged or weakly monitored assets such as edge devices, personal devices, and some third-party or virtual systems remain a common weak point because they often sit outside standard detection coverage. For executives, the implication is that response measured in hours is increasingly too slow. Focus should be on tighter identity controls, faster containment actions, better visibility of unmanaged exposure, and regular incident response drills so teams can act quickly when early warning signs appear.

Summary of last month's Cyber Alerts and News Clips:

Incident Response Solutions post certain alerts and tips we consider to be in the public interest as it comes to hand. We publish these alerts and tips on this webpage.

26/02/2026 - Exploitation of Cisco SD-WAN appliances

Our Views:

The Cyber Security Strategy 2026–2030 – Frontline Reality vs. Strategic Vision

The recently released New Zealand Cyber Security Strategy 2026–2030 and its accompanying Action Plan 2026–2027 set a vision for a New Zealand that "embraces cyber security to enable innovation, drive a prosperous economy and protect our digital way of life". Our views on this strategy are based on 24 years of experience responding to cybercrime incidents in New Zealand, including time with the NZ Police, Big4 consulting, and as a specialist digital forensic incident response (DFIR) firm. The content of this new strategy reflects exactly what we are seeing when responding to incidents on the ground.

The Strategy's data highlights the brutal reality for New Zealand businesses and individuals:

- Economic Impact: It is estimated that New Zealanders are losing more than $1.6 billion annually to cybercrime, primarily in the form of cyber-enabled fraud.
- Prevalence: In a survey of 295 large New Zealand businesses, 59% reported experiencing a cyber incident in the last year.
- National Significance: In 2025, 331 incidents were triaged for specialist technical support due to their potential national significance.

Objective 3: Respond and the Enforcement Gap

The Strategy's third objective, Respond, focuses on reacting effectively and decisively to adverse incidents. Key immediate actions identified in the plan include:

- Single Reporting Point: Establishing a single point for cyber incident reporting to improve data quality and access to recovery advice.
- Legislative Powers: Updating legislative powers to enable security sector agencies to use cyber capabilities to advance national security interests.
- International Cooperation: Working with partners to maintain lawful access while protecting personal data and privacy.

Regarding these actions, we observe the following:

- We note that while the Strategy prioritises the detection and disruption of high-impact threats , the immediate Action Plan remains at a high policy level regarding the specific enforcement required for common commercial crimes.
- We encourage the NZ government to consider the biggest impact to the cybercrime economy in New Zealand right now: Business Email Compromise (BEC) money mules.
- We encourage the government in its Action Plan to prioritise local enforcement, followed by police prosecutions and suitable deterrents set out by the courts, as this is key to reducing the impact of these operations.

Addressing the Insider Threat

The Strategy provides clear definitions for the threats we face:

- Cyber Incident: An event, intentional or not, that causes adverse consequences to an ICT system or its data.
- Cybercrime: Crimes committed through the use of computer systems and directed at computer systems.
- Cyber-enabled Crime: Crimes assisted, facilitated, or escalated in scale by the use of technology, such as online scams and fraud.

Regarding the scope of these threats, we observe the following:

- We note that the theft of sensitive intellectual property (IP) is identified as a national security challenge, yet the current Action Plan lacks specific initiatives to help businesses manage this risk.
- We note that the profile of this risk is increasing, with numerous cases of IP theft currently before the Employment Relations Authority (ERA) and the Employment Court.
- We encourage the NZ government in its Action Plan to consider if enough is being done to address the Insider Threat.
- We encourage the government to ensure businesses have the legislative and practical support necessary to protect their proprietary data from internal risks, alongside external cyber threats.

The 2026–2030 Strategy provides a solid framework, but its success will be measured by the transition from high-level policy to tangible enforcement and the protection of New Zealand's intellectual property and other at risk assets.

About the Bulletin:

The NZ Incident Response Bulletin is a monthly high-level executive summary containing some of the most important news articles that have been published on Forensic and Cyber Security matters during the last month. Also included are articles written by Incident Response Solutions, covering topical matters. Each article contains a brief summary and if possible, includes a linked reference on the web for detailed information. The purpose of this resource is to assist Executives in keeping up to date from a high-level perspective with a sample of the latest Forensic and Cyber Security news.

To subscribe or to submit a contribution for an upcoming Bulletin, please either visit https://incidentresponse.co.nz/bulletin or send an email to bulletin@incidentresponse.co.nz with the subject line either "Subscribe", "Unsubscribe", or if you think there is something worth reporting, "Contribution", along with the Webpage or URL in the contents. Access our Privacy Policy.

Subscribers to the premium edition also obtain access to the following additional information:

- Cyber Governance
- Cyber Incident Landscape
- Cyber Incident Response Resources
- Cyber Framework and Control Updates, Surveys and Research

Click here if you wish to subscribe to our Premium Edition of the Bulletin.

About Incident Response Solutions Limited:

Our Purpose - We help you with specialist forensic, cyber security and crisis management expertise at all stages throughout the incident response lifecycle.

Our Promise - We will provide you with the confidence you require to prepare, respond and recover from forensic and cyber incidents.

Our specialist Forensic Technology expertise includes Computer Forensics, Cybercrime Incident Response, Social Media Analysis and eDiscovery. We have significant experience in providing expert witness reports and in delivering expert witness testimony at trial. Our background includes experience in Law Enforcement (NZ Police) and Big 4 Professional Services.

Campbell McKenzie
Director
Incident Response Solutions Limited
0800 WITNESS
+64 21 779 310
campbell@incidentresponse.co.nz

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: