NZ Incident Response Bulletin

Standard Edition –February 2026 – Issue #85

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

Ministry review into the Manage My Health data breach

The Ministry of Health has set out the government's independent review with published Terms of Reference for the Manage My Health cybersecurity incident. It states the review is scheduled to commence on 30 January 2026 and anticipates a final report by 30 April 2026, while noting the Ministry will not provide public comment during the review period. For executives, the significance is twofold. First, the incident has moved into a structured assurance phase, signalling expectations of accountability, lessons learned, and measurable improvement actions. Second, it indicates heightened governance attention across health data handling and third-party platforms, where the outcome may affect procurement expectations, oversight models, and sector-wide cyber requirements. The linked Terms of Reference are also a useful reference point for what "good" looks like in incident review scope, evidence gathering, and decision-making scrutiny.

Recovery scams using phishing tactics to access bank accounts

The FMA warned about "recovery scams" that specifically target people who have already lost money to earlier scams. The playbook is to claim funds have been recovered, then direct victims to a website to "sign up" and enter personal details and online banking credentials, sometimes using New Zealand bank logos to look legitimate. Once credentials are captured, scammers can access accounts and transfer money out. For executives, this illustrates an important pattern: criminals increasingly exploit prior victim lists and public disclosures, meaning any incident (including non-financial ones) can produce downstream targeting of affected individuals. The FMA's advice focuses on resisting urgency, independently verifying who you are dealing with using official contact details, and contacting your bank immediately if credentials or payments have been shared. Organisations can reinforce this by communicating scam warnings after any breach, ensuring customer-facing teams can recognise and respond to these patterns, and strengthening MFA and anti-phishing protections for staff to reduce the chance of similar credential theft within the business.

Australia

Cyber expert gets rare Australian visa by hacking the government

British cybersecurity researcher Jacob Riggs secured Australia's highly selective National Innovation visa (subclass 858) after demonstrating real-world impact during his application. While awaiting a decision, Riggs tested a Department of Foreign Affairs and Trade (DFAT) system under DFAT's vulnerability disclosure framework, identified what he described as a "critical" issue (aligned with common severity scoring practices), and responsibly reported it. DFAT acknowledged the disclosure and added him to its public honour roll, providing verifiable evidence of technical achievement. The article positions the case as a non-traditional pathway to proving "exceptional talent", contrasting practical security outcomes with conventional credentials. For executives, the key message is that well-run vulnerability disclosure programs can materially improve security while also providing auditable proof of capability, and that immigration and talent programs may increasingly value demonstrated, measurable cyber impact over titles alone.

Major Australian gold producer confirms cyber attack

An ASX-listed gold producer confirmed it is investigating a cyber incident after a ransomware group's public listing suggested the company had been targeted. The company stated it detected unauthorised activity in mid-November 2025 and that automated security safeguards temporarily shut down and restricted access as a protective measure. It said a forensic investigation was initiated, relevant authorities were notified, and there was no operational or commercial impact. Importantly, the company reported it found no evidence that data was exported from its environment and stated it had not received any ransom demand. The report also notes that a subsidiary appeared on a ransomware leak site, but the threat actor provided limited detail, leaving uncertainty about whether any data theft occurred or whether ransomware was deployed. Overall, the key executive takeaway is that the organisation is treating the matter as a credible intrusion attempt, has completed initial containment and investigation steps, and is communicating that business operations and data exposure indicators remain negative at this stage.

World

Cyber risk in 2026: What executives must know about AI, fraud, geopolitics and more

The World Economic Forum argues that cyber risk is becoming systemic in 2026 as three forces converge faster than organisations can adapt: AI acceleration, geopolitical fragmentation and cyber-enabled fraud. It highlights survey findings from its Global Cybersecurity Outlook 2026, including that 94% of respondents see AI as the biggest driver of cyber change, with a shift in concern from "AI used by attackers" toward unintended data exposure from generative and agentic systems. Geopolitics is now a defining factor, with 64% of organisations accounting for geopolitically motivated attacks and prioritising threat intelligence and deeper engagement with governments. The article also states that fraud has overtaken ransomware as the top CEO concern, with 73% of respondents personally affected by cyber-enabled fraud in 2025. It flags persistent pressure points, especially third-party and supply chain exposure, skills shortages, and concentration risk in a small number of critical digital providers.

New Britain ransomware attack disrupts city systems for days, FBI investigating

New Britain, Connecticut officials confirmed a ransomware attack disrupted city network systems for more than 48 hours, forcing multiple departments to operate manually using pen and paper while investigators worked to restore services. The city said the outage began around 5 a.m. on Wednesday, when police were alerted to a network disruption that spread through the city's internet server, and it activated incident response protocols immediately. Federal and state authorities, including the FBI, are investigating, and the city engaged additional cyber security resources to secure systems and assess scope. Officials said it was too early to determine whether personal or confidential information on city servers was impacted. Despite disruptions affecting police and fire systems, leaders stressed public safety operations continued due to backup and manual redundancy plans, and essential services like plowing, trash collection, water, and sewer remained operational. The report highlights why municipalities are frequent targets: they have "no fail" missions and must keep services running even during major IT outages.

Data thieves borrow Nike's 'Just Do It' mantra, claim they ran off with 1.4TB

Nike is investigating a possible cybersecurity incident after the WorldLeaks extortion group claimed it stole a large trove of internal files (described as 1.4TB) and posted samples online. The material discussed appears to relate more to internal business operations, including design and manufacturing workflows, rather than customer account data. Nike has said it is assessing the situation but has not confirmed what data, if any, was taken or whether it would engage with any extortion demand. The story also reflects a broader criminal trend toward "steal-and-leak" extortion, where attackers focus on data theft and public pressure instead of encrypting systems. For executives, the main risk is commercial and operational sensitivity: exposure of product development, supplier, or production documentation can enable competitive intelligence, counterfeit activity, and partner trust issues, even if core services remain unaffected. The immediate priorities are validating the data's authenticity, scoping impact, containing access, and preparing for follow-on reputational and phishing risks.

'We're losing massively': EU cyber chief warns Europe's defenses lag

POLITICO reports that ENISA Executive Director Juhan Lepassaar is urging the EU to fundamentally rethink its cyber defenses because the scale and speed of attacks are outpacing current investment and capacity. He argues Europe is "losing" against hackers, citing major disruptive incidents across airports, elections and hospitals, and highlighting stark threat metrics, including Germany's Bundesbank reporting thousands of attacks per minute. Lepassaar links the growing risk to a surge in reported software vulnerabilities (rising from roughly 17,000 in 2019 to over 41,000 in 2025) and dramatically shorter "time to exploit", shrinking from around two months to about one day, accelerated in part by AI. While the European Commission has proposed revising the Cybersecurity Act and expanding ENISA staffing, Lepassaar says this is insufficient and calls for EU-level cyber infrastructure, with at least a doubling of capability.

Latvia says Russia remains its top cyber threat as attacks hit record high

Latvia's national security service (SAB) warns that Russia remains the country's primary cyber threat, even as many incidents have not caused major disruption. In its annual report, SAB says 2025 saw a record high in registered cyber threats, rising well above pre-2022 levels. While much of the activity is attributed to cybercrime and digital fraud rather than direct critical infrastructure compromise, the agency highlights more serious cases including intrusion attempts, malware distribution, equipment compromise, and DDoS attacks. SAB links the persistent risk to Latvia's political, military, and material support for Ukraine, and notes that Russian-linked hacktivist groups have demonstrated willingness and capability to target operational technology and industrial control systems, often aiming for short-term disruption and intimidation. DDoS activity against government and critical services is reported to spike around politically sensitive events. SAB concludes the threat from Russia is likely to remain high into 2026 and beyond.

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.

30/01/2026 – CVE-2026-24061 affecting GNU InetUtils

Our Views:

When the Dust Settles: What Inquiries Reveal About Cyber Readiness

Incident preparation is often framed as a technical exercise: build playbooks, buy tooling, run a tabletop, hope for the best. But when you read the output of an inquiry or the reasoning in a prosecution, a different picture emerges. The question is rarely "did you have a plan". It is "was your organisation governing cyber risk in a way that made the incident less likely, less severe, and handled in a way that limited harm once things went wrong".

That is why inquiries like the review into the Manage My Health (MMH) incident, and prosecutions such as the Australian Clinical Labs (ACL) matter as preparation inputs. They show what gets attention when scrutiny is applied. Not in the abstract, but in the lived reality of a breach: competing priorities, imperfect information, and decisions made under pressure.

A consistent lesson is that post-incident scrutiny does not stop at the point of compromise. Reviewers and regulators look backward and forward. Backward, to understand whether risk was being actively identified and reduced. Forward, to assess whether response decisions were made quickly, coordinated properly, and communicated in a way that supported those affected. The MMH inquiry framing reinforces that the scope is bigger than the vulnerability itself. It includes whether protections were adequate, whether known issues were acted on, how well response processes worked, and what that means for similar services across the sector. The ACL case, in turn, underscores that "reasonable steps" is assessed objectively and that response obligations can be viewed separately from the underlying security failure.

For governance teams, that shift in emphasis is important. It means your preparation cannot be limited to incident response mechanics. You need to be able to demonstrate that governance was functioning before the incident, and that it supported timely, defensible decisions during it.

In practice, this comes down to evidence. After a serious incident, it is common for organisations to talk about what they "intended" to do, what they "normally" do, or what they were "about to" implement. That rarely lands well. The more persuasive story is the one you can prove: how risks were assessed, how controls were selected, how assurance was performed, and how findings were tracked through to completion or formally accepted. Inquiries like MMH draw attention to whether audit or security warnings were acted upon. Courts and regulators, as in ACL, look for tangible indicators that security steps were appropriate for the sensitivity of the information and the threat environment.

The second theme is speed and structure once suspicion arises. A lot of organisations invest heavily in detection and containment, but underinvest in the governance mechanics that follow. Who decides whether an event is likely to create serious harm. What triggers external notification. How legal, privacy and communications functions are brought in without slowing down the technical response. Which decisions must be documented and by whom. ACL is a useful reminder that delays or confusion around assessment and notification can become part of the core issue, not a side note. The message for preparation is simple: treat the "assessment to notification" pathway as a governed process, not an improvised meeting.

There is also a sector-wide angle that comes through strongly in inquiries. When services are integrated, when data moves between systems, and when platforms are shared, a single incident quickly becomes a question about wider exposure. That kind of review lens makes organisations ask a better preparation question: "If this happened to us, would we know where else the same weakness might exist, and could we check quickly". That requires more than good intentions. It requires up-to-date system visibility, clear ownership across integrated environments, and a repeatable method for validating controls across similar assets.

Perhaps the most useful way to think about all this is to treat incident preparation as governance readiness. Could you confidently brief your board with a clear account of what you knew, when you knew it, what you decided, and why. Could you show how cyber risk is reported and managed, how exceptions are approved, how assurance is performed, and how you confirm that security improvements actually stick. Could you demonstrate that your organisation's "reasonable steps" are aligned to the nature of your data, your operating context, and the reality of modern threats.

If you can, you are not just prepared to respond to an incident. You are prepared for what follows it. And that is increasingly the standard that matters.

If you want to harden that governance posture after an incident (or a major exercise), our Cyber Post-Incident Review service is designed to turn response activity into measurable resilience. We help reconstruct a defensible timeline, identify root causes (not just symptoms), assess what worked and what failed across technical and business response, and translate findings into actionable recommendations that leadership can track through to completion.

NZ Incident Response Bulletin

Standard Edition –February 2026 – Issue #85

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

This Bulletin is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained within this Bulletin. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, when relying on the information contained in this Bulletin or for any decision based on it.

Further Resources:

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

Share our Bulletin: