NZ Incident Response Bulletin

Premium Edition – October 2025 – Issue #81

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

More than half of New Zealand businesses experiencing cyber threats

More than half of New Zealand businesses reported experiencing cyber threats in the past year, according to a 2025 survey conducted by the National Cyber Security Centre (NCSC). The survey, which included responses from over 300 medium-to-large organisations, found that 56% had encountered at least one cybersecurity incident. The findings highlight a growing threat environment, with phishing, ransomware, and supply chain attacks among the most commonly reported issues. Despite these risks, only 59% of respondents said they were confident in their organisation's ability to respond effectively to cyber incidents. The report stresses the importance of governance and leadership engagement in cybersecurity, noting that board-level oversight and clear cyber risk ownership significantly improve resilience. The NCSC recommends adopting a proactive approach, including regular incident response planning, staff awareness training, and implementing baseline security controls. The survey aims to inform both public and private sector strategies for enhancing national cyber resilience.

New Zealand strengthens Russian oil price cap

In September 2025, the New Zealand Government expanded its sanctions regime against Russia, reinforcing international efforts to limit Moscow's ability to fund its war in Ukraine. Notably, the announcement includes new cyber-related sanctions targeting entities and individuals involved in malware and cyber operations against Ukrainian government networks. While the broader package focuses on aligning with G7-led oil price caps and financial restrictions, the cyber-specific measures reflect Wellington's recognition of digital threats as a core part of hybrid warfare. This is part of an ongoing commitment under the Russia Sanctions Act 2022. Foreign Minister Winston Peters noted the importance of holding cyber actors accountable and disrupting malicious state-linked capabilities. This action complements prior designations of Russian military and technology firms and signals a broader integration of cyber response into NZ's foreign policy toolkit.

Reti earmarks $70m of new agency's budget for AI commercialisation grants

New Zealand's Minister for Technology and AI, Shane Reti, announced that $70 million from the upcoming New Zealand Institute for Advanced Technology will be allocated toward AI commercialisation grants over the next seven years. This funding is part of a broader strategy to enhance New Zealand's capability in artificial intelligence, with a focus on supporting startups and businesses to scale AI solutions domestically and globally. The grants aim to accelerate innovation, attract private sector investment, and ensure New Zealand keeps pace with international developments in AI. Reti emphasised the need to build "world-class expertise" in areas like machine learning and data science while ensuring ethical governance. The agency, expected to be operational by early 2026, will serve as a key pillar in the government's emerging tech strategy. The move signals growing recognition that AI has significant economic, strategic, and security implications for New Zealand's digital future.

Australia

Three dead in Australia after Optus glitch disrupts emergency calls

A major Optus outage on 18 September 2025 severed routing for Triple Zero (000) emergency calls, causing 600+ failures and contributing to three deaths across Australia. Caused by a routine firewall upgrade, the incident prompted immediate government criticism over Optus's delayed notifications and lack of planning. Formal inquiries by ACMA and the Department of Communications are underway, highlighting the urgent need for better incident response and regulatory reform for critical infrastructure.

Software owned by Australian banks being tested for social media ban

Australia is testing bank-developed identity tools (like ConnectID) to enforce a national ban on social media for under-16s starting December 2025. These tools will verify users' ages before they can access platforms like Instagram and TikTok. While crucial for compliance, the move raises privacy concerns over linking financial identity systems to social media use. This signals a precedent for using banks' digital identity infrastructure in broader digital regulation.

World

Airport chaos highlights rise in high-profile ransomware attacks, cyber experts say

In late September 2025, global ransomware activity surged, marked by high-profile incidents and evolving attack techniques. A ransomware attack on Collins Aerospace's vMUSE system disrupted airport check-in and baggage services across Europe, illustrating attackers' focus on critical infrastructure for maximum impact. Worldwide, ransomware attacks have spiked 36% compared to 2024, with 24% of organisations reporting incidents this year. This resurgence is driven by more sophisticated methods, including AI-powered phishing and credential theft. The LockBit group re-emerged with a more advanced LockBit 5.0 variant, offering cross-platform capabilities and enhanced anti-analysis features. Researchers also flagged the rise of "Ransomware 3.0," where large language models dynamically generate malware components, enabling greater flexibility and detection evasion. These trends indicate that ransomware threats are intensifying both in scale and complexity. Experts stress the need for comprehensive resilience measures, including zero trust architectures, continuous threat monitoring, and robust incident response plans to counter these evolving risks.

Heathrow: UK police arrest man after airports targeted in cyber attack

UK authorities arrested a 30-year-old man at Heathrow Airport in September 2025 on suspicion of launching cyberattacks that disrupted online services for multiple UK airports, including London City, Manchester, and Stansted. While no flight operations were affected, the cyberattacks — reportedly distributed denial-of-service (DDoS) campaigns — temporarily knocked public websites offline, drawing attention to vulnerabilities in aviation-sector digital infrastructure. The arrest was made under the UK's Computer Misuse Act, and the suspect was taken into custody at London's Heathrow Airport. Investigators are examining links to Russian-aligned hacktivist groups who had previously claimed responsibility for similar disruptions. The case highlights increasing use of cyberattacks as tools of geopolitical influence and protest, with critical infrastructure — particularly transport — becoming a frequent target.

Two teenagers charged over Transport for London cyber attack

Two teenagers have been charged with conspiracy to commit unauthorised acts against Transport for London (TfL) following a massive cyber attack that caused £39 million in damages and three months of disruption. The NCA believes the hack, which began in August last year, was conducted by members of the Scattered Spider group. The incident severely impacted TfL's online services and information boards. Approximately 5,000 customers were notified that personal data, including bank details, may have been accessed. One of the charged individuals also faces allegations of targeting US healthcare companies.

'You'll never need to work again': Criminals offer reporter money to hack BBC

A BBC cyber correspondent was contacted by the ransomware group Medusa and offered a cut of a potential multi-million-pound payout for insider access to BBC systems. The hacker, identifying as "Syn," offered 25% of the ransom to the reporter for their login details, promising they "wouldn't need to work ever again." When the reporter stalled, the criminals escalated with an MFA (Multi-Factor Authentication) bombing attack on the reporter's phone. This forced the reporter's account to be disconnected from the BBC network as a security precaution. The incident highlights the growing threat of insider coercion used by cyber-criminal groups.

Asahi stops pouring after cyberattack stops production

In September 2025, Asahi Group, one of Japan's largest beverage companies, was forced to halt beer production due to a cyberattack that disrupted its IT systems. The incident, which affected several of the company's domestic breweries, also impacted logistics and order processing. While the full details of the attack have not been publicly disclosed, it is suspected to involve ransomware. Asahi reported that no customer or supplier data was compromised, but the operational disruption significantly affected supply chains and delivery schedules. The company activated its business continuity plan and engaged cybersecurity specialists to investigate and restore systems. This event highlights the growing vulnerability of manufacturing and supply chain operations to cyberattacks, particularly as industrial systems become more digitised. It also underscores the need for the food and beverage sector to enhance its cybersecurity resilience, including network segmentation, regular backups, and monitoring of operational technology environments for anomalies or intrusions.

UK government will underwrite £1.5bn loan guarantee to Jaguar Land Rover after cyber-attack

In September 2025, Jaguar Land Rover (JLR) faced significant disruption due to a cyberattack that halted engine manufacturing operations. The attack targeted IT systems supporting production, prompting the company to suspend activities at its key engine plant in Wolverhampton, UK. As a result, production lines for vehicles reliant on these engines, including the Range Rover and Defender, experienced knock-on effects. JLR has since announced plans to restart operations in early October after implementing security and recovery measures. The UK government has stepped in with a £1.5 billion loan guarantee to support the company's recovery and supply chain continuity, underlining the incident's economic and industrial significance. While specific details of the cyberattack remain undisclosed, it highlights the vulnerability of manufacturing operations to cyber threats and the critical need for cyber resilience across operational technology (OT) environments. The event underscores broader concerns about national industrial cybersecurity and supply chain robustness amid rising global threats.

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.

26/09/2025 - Multiple vulnerabilities affecting Cisco ASA devices

Our Views:

Cyber Smart Week NZ: Emphasizing the Human Factor in Security

This Cyber Smart Week, it's timely to reflect on an uncomfortable truth: many cyber incidents originate due to human factors. Verizon's 2025 Data Breach Investigations Report (DBIR) reviewed over 22,000 security incidents and concluded that roughly 60 percent of confirmed breaches involved a human element — deliberate or accidental. In short: employees clicking a phishing link, misconfiguring access, or failing to spot deception remain a dominant threat vector.

Those human-factor statistics feed directly into frameworks like the CIS Critical Security Controls. The CIS community, which maps its controls to real-world threat data, uses such findings to justify investing in the human side of security — not just firewalls and endpoint protection.

CIS Control 14: Security Awareness and Skills Training

Among the CIS Controls, **Control 14** is dedicated entirely to training and awareness. It acknowledges that technology alone won't prevent every attack — people need to know how to spot threats, act safely, and respond to anomalies.

Within Control 14, **Safeguard 14.9**— *Conduct Role-Specific Security Awareness and Skills Training* — is especially important. This isn't generic "cyber hygiene for all" training. Instead, it demands that training speaks meaningfully to an individual's role and risk exposure, such as:

- Developers get training on secure coding, input validation, and common web vulnerabilities.
- Finance teams learn to spot invoice fraud, social engineering tied to payments, and red flags in approval workflows.
- Executives and board members receive briefings on impersonation attacks, insider manipulation, and decision-making under duress.

Role-specific training closes critical gaps attackers love to exploit. When people are trained in the particular threats that affect their day-to-day work, the "human factor" becomes less of a weakness and more of an active defense.

Why Following These Controls Matters

From our work with clients, there's a clear pattern: organisations that implement Control 14 (especially 14.9) *consistently* show stronger resilience. They:

- Detect phishing or internal misbehavior earlier
- Report suspicious events more freely
- Maintain higher overall vigilance, making lateral attacks harder to execute

In fact, firms that train by role tend to have fewer repeat incidents and lower remediation costs. It's not a guarantee — security is never perfect — but it's a demonstrable difference. The training builds the muscle memory and mindset that prevent small mistakes from cascading into full breaches.

When staff understand *why* certain requests are suspicious, they're less likely to blindly comply. That intuition alone closes many attack pathways before technology even needs to respond.

National Initiatives: Strength in Collective Awareness

Beyond what individual organisations do, national programs help raise the baseline of cyber awareness. In New Zealand, **Cyber Smart Week 2025** aims to bring that lift: helping citizens, small businesses, public services and families understand their online risks and defences. The government is hosting a webinar series to deliver free, practical sessions for all levels of tech comfort. Programmes like this matter because they help shift the culture. If more people understand phishing, secure passwords, and report scams, then attackers face a harder environment. What's a "trickle-up" effect: when even non-technical users push back, the weakest links in an attack chain get stronger.

Our New Fraud Training Module: Bridging Cyber & Financial Risk

To help clients meet the requirements of Control 14 (and Safeguard 14.9), we've developed a specialised Fraud Risk Management module on our CyberSafeHQ platform, currently free for individual enrolment. This module does more than just teach "don't click suspicious links." It layers in scenarios around insider fraud, payment manipulation, vendor scams, and executive impersonation. You can also check out the latest AI video content creation from Google Veo, to help you spot deepfakes!

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: