NZ Incident Response Bulletin

Standard Edition – May 2025 – Issue #76

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.

Not subscribed to our Premium Bulletin? Click here to join

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

NZ banks introduce new fraud protections, will reimburse scam victims up to $500,000

New Zealand banks announced significant enhancements to their fraud protection measures, including a commitment to reimburse scam victims up to $500,000. Effective from 30 November 2025, these changes are part of an updated Code of Banking Practice aimed at strengthening consumer safeguards. The new measures encompass advanced technologies to detect risky transactions, the ability to freeze suspect accounts, and the implementation of a "confirmation of payee" service to ensure the recipient's name matches the account number. Additionally, banks will provide pre-transaction warnings for high-risk payments and establish a 24/7 reporting channel for suspected scams. Reimbursement will be contingent upon the bank's failure to meet these prevention commitments and the customer's exercise of reasonable care. These initiatives align New Zealand's banking practices with international standards, reflecting a proactive approach to combating the growing threat of financial scams.

Defence Ministry puts out tender for help strengthening systems 'increasingly vulnerable' to cyber attack

The New Zealand Ministry of Defence has issued a tender, seeking assistance to enhance its cybersecurity infrastructure, acknowledging that its systems are "increasingly vulnerable" to cyberattacks. As part of a broader $12 billion Defence Capability Plan, the Ministry plans to allocate between $100 million and $300 million over the next four years specifically for cyber upgrades. The initial phase, termed the Cyber Security and Support Capability programme, aims to procure technologies such as a threat intelligence platform and a planning system. The Ministry emphasizes the growing threat landscape due to increased digital integration and seeks assurances from bidders regarding the origin of equipment and the security measures in place for their installation. Operating under financial constraints, the Ministry is focused on obtaining maximum value for money while ensuring that its cyber-connected capabilities are robust enough to maintain its status as a credible and trusted partner.

'A sense of invisibility' - Lack of Government leadership, cyber-security big concerns in TUANZ survey of business leaders

The TUANZ Digital Priorities 2025 report, based on interviews with CIOs from major New Zealand organizations, highlights significant concerns over the government's perceived lack of leadership in digital transformation. Business leaders express disappointment, citing a "sense of invisibility" regarding governmental support and strategy in advancing digital initiatives. Despite initial enthusiasm from the current administration, many feel that tangible actions and policies have not materialized, leaving a strategic void in areas like AI governance and cybersecurity. Cybersecurity emerges as a top priority, especially given New Zealand's declining rankings in global cybersecurity and privacy protection indices. Leaders advocate for a cohesive national digital strategy, emphasizing the need for bipartisan support and proactive measures to address evolving technological challenges and to foster innovation across sectors.

Australia

Banking passwords stolen from Australians are being traded online by cybercriminals

A recent investigation by cybersecurity firm Dvuln has uncovered that over 31,000 banking credentials from Australian customers of the Big Four banks - Commonwealth Bank, ANZ, NAB, and Westpac - are being traded on platforms like Telegram and the dark web. These credentials were harvested through "infostealer" malware, which infects users' personal devices, predominantly Windows systems, to extract sensitive data such as passwords, credit card details, and browser information. Notably, this breach stems from compromised personal devices rather than vulnerabilities within the banks' systems. The malware's stealthy nature allows it to remain undetected for extended periods, continuously siphoning updated information to cybercriminals. Experts warn that even multi-factor authentication can be bypassed if authentication tokens are compromised. This situation underscores the critical need for individuals to maintain updated security software, exercise caution with downloads, and regularly monitor their accounts for suspicious activity. The Australian Signals Directorate has termed this widespread issue the "silent heist," highlighting the escalating threat of such cyberattacks.

Hackers strike Australia's largest pension funds in coordinated attacks

In April 2025, Australia's retirement savings sector, valued at A$4.2 trillion, experienced coordinated cyberattacks targeting major pension funds, including AustralianSuper, Australian Retirement Trust (ART), Rest Super, Insignia Financial, and Hostplus. AustralianSuper, managing A$365 billion for 3.5 million members, reported that up to 600 accounts were compromised, resulting in four members losing a total of A$500,000. Rest Super detected unauthorized access to approximately 20,000 accounts, prompting an immediate shutdown of its member portal. ART and Insignia Financial observed unusual login activities but reported no financial losses. National Cyber Security Coordinator Michelle McGuinness is leading a comprehensive response involving government agencies, regulators, and industry stakeholders. Prime Minister Anthony Albanese emphasized the frequency of such cyber threats, noting that attacks occur approximately every six minutes in Australia.

AFP joins forces with Philippines to crack down on offshore scammers

The Australian Federal Police (AFP) is collaborating with Philippine authorities under Operation Firestorm to disrupt scam operations targeting Australians. These “boiler room” scam centres, based in the Philippines, use tactics like romance and investment fraud to extract billions from victims—Australians alone lost over $2 billion in the past year, with investment scams comprising nearly half. AFP officers are training Philippine law enforcement, including the Presidential Anti-Organised Crime Commission and the Cyber Crime Division, to detect, raid, and dismantle these offshore cybercrime hubs. The initiative has already resulted in hundreds of arrests and the seizure of critical digital evidence.

World

Law firm fined £60,000 following cyber attack

The UK's Information Commissioner's Office (ICO) fined Merseyside-based DPP Law Ltd £60,000 for a significant data breach resulting from a June 2022 cyberattack. Attackers exploited an infrequently used administrator account lacking multi-factor authentication to access the firm's legacy case management system, exfiltrating over 32GB of sensitive client data, including legally privileged information. DPP Law only became aware of the breach when the National Crime Agency informed them that client data had surfaced on the dark web. Despite the breach's severity, the firm delayed reporting the incident to the ICO by 43 days, exceeding the 72-hour requirement under the UK General Data Protection Regulation (UK GDPR). The ICO's investigation highlighted DPP Law's failure to implement adequate security measures, such as MFA and timely vulnerability patching, underscoring the legal obligation for organisations to proactively safeguard personal data and promptly report breaches to mitigate potential harm.

X’s use of European user data for Grok may have breached the GDPR

Elon Musk's social media platform X (formerly Twitter) is under investigation by Ireland's Data Protection Commission (DPC) for potentially breaching the EU's General Data Protection Regulation (GDPR). The probe centers on allegations that X used publicly accessible posts from European users to train its AI chatbot, Grok, without obtaining explicit consent. In May 2024, X implemented a default setting that permitted the use of user data for AI training, requiring users to opt out manually—a practice that may violate GDPR's consent requirements. Although X agreed to halt this data processing following legal action, the DPC's inquiry continues, with the authority to impose fines up to 4% of X's global revenue. This case underscores the increasing regulatory scrutiny over AI data practices and the importance of transparent user consent mechanisms in compliance with data protection laws.

South Korea says DeepSeek transferred user data to China and the U.S. without consent

South Korea's Personal Information Protection Commission (PIPC) determined that DeepSeek, a Chinese AI chatbot, had transferred personal data of over one million South Korean users to China and the U.S. without obtaining proper consent. This data included sensitive information such as chat histories, device identifiers, and behavioral patterns, raising significant privacy concerns. In response, the PIPC suspended new downloads of the DeepSeek app within South Korea until the company addressed these violations. DeepSeek acknowledged shortcomings in complying with South Korea's data protection laws and appointed local legal representatives to facilitate remediation. This incident underscores the critical importance of stringent data governance and transparency, especially for AI applications handling vast amounts of personal information across borders.

Cybercriminals and scammers stole a record $16B in 2024, new FBI report says

In 2024, Americans reported a record $16.6 billion in losses from cybercrime, marking a 33% increase over the previous year, according to the FBI's Internet Crime Complaint Center (IC3) . Despite a slight decrease in the number of complaints to 859,532, the financial impact intensified, highlighting the growing sophistication of cybercriminals. Phishing, extortion, and personal data breaches were the most reported crimes, while investment fraud—particularly involving cryptocurrencies—accounted for over $6.5 billion in losses. Individuals aged 60 and older were disproportionately affected, filing 147,127 complaints and incurring nearly $5 billion in losses .

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.

Our Views

Evolving Incident Response – Key Updates from NIST SP 800-61r3

Overview
The National Institute of Standards and Technology (NIST) has released a significant update to its guidance on cybersecurity incident response. The transition from **SP 800-61 Revision 2 (2012)** to **SP 800-61 Revision 3 (April 2025)** reflects a strategic evolution, moving away from a reactive posture and toward integration with NIST Cybersecurity Framework (CSF) 2.0. This shift acknowledges the increasing complexity and persistence of cyber threats and underscores the need for response strategies to be embedded within an organisation's broader risk management practices.

Why It Matters for New Zealand Organisations
In recent years, several high-profile cyber incidents across New Zealand have highlighted critical gaps in incident readiness and response agility. These events demonstrated how delays in detection, unclear escalation paths, and fragmented stakeholder communication can lead to prolonged disruption and reputational damage. Conversely, other organisations that had mature incident response plans – including playbooks aligned to risk tiers, executive visibility, and pre-established coordination with legal and communications teams – were able to limit the impact, reduce downtime, and maintain public trust.

No one industry is immune from cyber-attacks, although we see professional services as lagging behind in cyber incident preparedness given, they amongst the highest targeted. The adoption of structured and up-to-date incident response practices is essential to national cyber resilience. The updates in SP 800-61r3 offer a timely opportunity for New Zealand organisations to reassess their preparedness and align with global best practices.

Key Enhancements in SP 800-61r3

- **CSF 2.0 Alignment:**
  Incident response is mapped to the six CSF 2.0 Functions – Govern, Identify, Protect, Detect, Respond, and Recover – promoting a lifecycle approach that incorporates governance and strategic risk management.

- **Focus on Continuous Improvement:**
  The guidance stresses the importance of learning from every incident, embedding insights into planning, training, and control updates.

- **Broadened Stakeholder Involvement:**
  Successful incident response is shown to depend on inclusive coordination across executive leadership, legal, HR, IT, and external partners.

- **Dynamic Resources:**
  SP 800-61r3 points organisations to online tools like the **Cybersecurity and Privacy Reference Tool (CPRT)** for evolving guidance in real-time.

Evaluate Incident Response Maturity

NIST SP 800-61r3 presents a forward-thinking framework that moves incident response from a reactive function to a core component of strategic risk management. We recommend New Zealand organisations review this guidance to help build resilience, minimise disruption, and ensure coordinated, effective responses in an increasingly hostile cyber threat environment. The follow are three essential steps to being with:

Benchmark: Begin by benchmarking your organisation's existing incident response (IR) capabilities against an established framework. Focus not only on technical capabilities but also on governance, roles, escalation paths, and decision-making processes. Pay close attention to areas such as threat detection, response coordination, and executive oversight. Prioritise improvements in domains where there is limited visibility, unclear accountability, or inconsistent documentation. This assessment should also consider third-party and supply chain dependencies, which are increasingly common vectors in major breaches.

Simulate and Train: Conduct regular, realistic tabletop exercises that bring together executives, operational teams, legal, communications, and relevant third parties. Scenarios should reflect the types of incidents most relevant to your organisation's risk profile - such as ransomware, data breaches, or cloud service compromise. Ensure exercises test both technical containment procedures and business continuity impacts. These simulations should be reviewed post-exercise with formal after-action reports, highlighting gaps, miscommunications, or areas where decisions were delayed or unclear.

Institutionalise Post-Incident Learning: Establish a structured post-incident review process that activates after every incident - regardless of severity. Ensure the process captures technical findings, response timelines, coordination issues, and decision points. Engage all stakeholders involved, from security teams to executive sponsors, to review outcomes and agree on follow-up actions. Lessons learned should directly inform updates to IR playbooks, awareness training, system configurations, and business continuity plans. Embedding this feedback loop ensures continuous improvement and resilience-building over time.

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: