NZ Incident Response Bulletin

Premium Edition – June 2025 – Issue #77

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

Cyber attacks cost Kiwis an estimated $1.6 billion in 2024

A report from the National Cyber Security Centre (NCSC) revealed that New Zealanders suffered approximately NZD $1.6 billion in financial losses due to online threats in 2024. The study found that 54% of adults experienced some form of cyber threat in the last six months of the year, with around 830,000 individuals incurring financial losses averaging $1,260 per incident. Despite the significant impact, underreporting remains a concern, with 44% of victims not reporting incidents, often due to embarrassment or lack of awareness about reporting channels. The NCSC emphasized the importance of proactive cybersecurity measures, such as enabling two-factor authentication and using password managers, to mitigate risks.

Budget 2025: Spy agencies funds cut as security threats grow

New Zealand's 2025 Budget includes funding reductions for the country's core intelligence agencies—the GCSB sees its budget decrease to NZ$267 million (down approximately 20%), and the NZSIS drops from NZ$117 million to NZ$111 million. These cuts come at a time when national security threats such as cyber attacks, foreign interference, extremism, and espionage are on the rise. The government has explained that the reductions are due to the conclusion of a major capital project rather than a reassessment of priorities. Both intelligence agencies have stated they remain sufficiently resourced to meet operational requirements. The cuts occur against a backdrop of regional instability and growing global tensions, particularly in the Indo-Pacific. In contrast, other Five Eyes nations like Australia, the UK, and Canada are increasing intelligence funding, although the U.S. is making cuts. These changes follow a 2023 fiscal efficiency initiative that saved NZ$11 million, with Budget 2025 avoiding additional reductions.

More people worried about impact of technology on privacy - survey

An annual survey by the Privacy Commissioner revealed that public concern about privacy remains high, with particular unease around children's privacy, social media use, and the use of artificial intelligence in decision-making. Nearly half of respondents reported increased concern over the past few years, and over 80% expressed a desire for more control over their personal information. The findings underscore the need for organizations to adopt transparent data practices and prioritize data minimization to build public trust.

Australia

Boards have a tougher choice to make from today if they get hacked

Australian companies face heightened responsibilities under new cybersecurity regulations mandating the disclosure of ransom payments to cybercriminals. Organizations with an annual turnover exceeding AUD $3 million, or those classified as critical infrastructure, are now required to report any ransom payments within three days via an online portal managed by the Department of Home Affairs and the Australian Signals Directorate. This development places increased pressure on company boards, compelling them to navigate complex decisions regarding ransom payments, which may involve legal, ethical, and reputational considerations. The mandatory reporting aims to enhance government visibility into cyber threats and inform national cybersecurity strategies. However, it also introduces potential challenges, such as public scrutiny and legal implications, thereby necessitating robust incident response plans and board-level engagement in cybersecurity governance. This regulatory shift underscores the critical importance of proactive cybersecurity measures and transparent risk management practices within Australian enterprises.

Cybercriminals steal nearly 100 staff logins at Australia's Big Four banks

Cybersecurity experts reported that cybercriminals had compromised nearly 100 staff logins from employees at Australia's Big Four banks—Commonwealth Bank, ANZ, NAB, and Westpac. The attackers used "infostealer" malware to harvest credentials from workers' devices, subsequently sharing them online. Although the banks have implemented protective measures to prevent unauthorized access, the exposure of these credentials heightens the risk of data breaches and ransomware attacks. Security analysts warn that such breaches could allow attackers to infiltrate corporate networks, emphasizing the need for robust cybersecurity protocols and employee awareness to mitigate potential threats.

NSW government to introduce new laws to target 'scourge' of cybercrime fraud

The New South Wales (NSW) government is set to introduce the Identity Protection and Recovery Bill to combat identity theft and cybercrime, which cost Australians approximately $2 billion in 2024. The legislation will establish a fraud check service and a Compromised Credential Register, allowing government and accredited agencies to verify if an individual's identity documents have been stolen or compromised. This initiative aims to prevent the misuse of personal information in fraudulent applications for grants or credit. It will also empower ID Support NSW to serve as the main government provider for identity protection and recovery.

World

Russia accused of trying to hack border security cameras to disrupt Ukraine aid

A coalition of Western intelligence agencies, including those from the UK, US, Germany, and France, disclosed a comprehensive Russian cyber-espionage campaign targeting the logistics of military and humanitarian aid to Ukraine. The operation, attributed to Russia's GRU Unit 26165 (also known as Fancy Bear or APT28), involved compromising over 10,000 internet-connected cameras situated at critical transit points such as border crossings, rail stations, and military installations across Ukraine and neighbouring countries including Romania, Poland, Hungary, and Slovakia. These breaches provided Russian operatives with real-time surveillance capabilities to monitor aid movements. Additionally, the campaign employed spear-phishing emails—often containing adult content or spoofed professional information—and voice phishing tactics to infiltrate organizations involved in aid delivery. By accessing sensitive logistics data, including shipping manifests and transit schedules, the attackers aimed to gather intelligence that could be used to disrupt the flow of support to Ukraine.

US probes effort to impersonate White House chief of staff

U.S. federal authorities initiated an investigation into a cybersecurity incident involving the impersonation of White House Chief of Staff Susie Wiles. According to the Wall Street Journal, Wiles reported that her personal cell phone contacts had been compromised, enabling an impersonator to access private phone numbers. This breach led to fraudulent communications being sent to high-profile individuals, including senators, governors, and top business executives, from someone claiming to be Wiles. The incident affected her personal device, not her government-issued phone. The FBI emphasized the seriousness of threats against presidential staff and the importance of secure communication channels. This event follows previous cybersecurity challenges within the White House, including a breach of communications used by former National Security Adviser Mike Waltz and a reported Chinese cyber-espionage campaign known as "Salt Typhoon," which targeted senior U.S. political figures. Given Wiles' prominent role in the administration, her personal data is considered a valuable target for foreign intelligence agencies and other hostile actors.

Czech Republic Accuses China of Cyberattack on Foreign Ministry

The Czech Republic has accused China of orchestrating a cyber attack on its foreign ministry's unclassified communications network, attributing the action to the state-sponsored hacking group APT31, associated with the Chinese Ministry of State Security. Foreign Minister Jan Lipavský condemned the interference and summoned China's ambassador. While the extent of the impact was not disclosed, a new communications system has been implemented. NATO reported that the attack caused "damage and disruption," and, along with the EU, strongly condemned the incident, calling it a violation of international norms. This attack is consistent with previous allegations against APT31, which has been linked by the U.S. and U.K. to attacks on political institutions. Another group, APT40, has also been implicated in global cyber espionage efforts under Beijing's directive. Czech officials have shared incident data with EU, NATO, and Indo-Pacific partners. Prague's pro-Taiwan stance may have contributed to tensions, especially after Czech President Petr Pavel became the first elected European leader to speak with Taiwan's president. Beijing has not responded to the latest accusation but has denied similar allegations in the past.

ConnectWise Hit by Cyberattack; Nation-State Actor Suspected in Targeted Breach

ConnectWise, the developer of remote access and support software ScreenConnect, has disclosed that it was the victim of a cyber attack that it said was likely perpetrated by a nation-state threat actor. "ConnectWise recently learned of suspicious activity within our environment that we believe was tied to a sophisticated nation-state actor, which affected a very small number of ScreenConnect customers," the company said in a brief advisory on May 28, 2025. The company said it has engaged the services of Google Mandiant to conduct a forensic probe into the incident and that it has notified all affected customers. However, it did not reveal the exact number of customers who were impacted by the hack, when it happened, or the identity of the threat actor behind it.

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.

27/05/2025 – Guidance for SIEM and SOAR Implementation

23/05/2025 – Joint Cybersecurity Information AI Data Security – Best Practices for Securing Data Used to Train & Operate AI Systems

6/05/2025 – Primary Mitigations to Reduce Cyber Threats to Operational Technology

Our Views:

Preventing and Managing Accidental Sensitive Data Leaks to Generative AI

Generative AI (GenAI) platforms like ChatGPT offer powerful productivity benefits, but they also introduce new risks when employees accidentally feed sensitive or proprietary data into them. Recent incidents (such as employees unwittingly leaking confidential source code via ChatGPT) have spotlighted the potential fallout. For organisations in New Zealand, it's imperative to understand these risks, have a response plan, and implement preventative measures. Emphasis and effort should be focused on risk mitigation, strong governance, and compliance with NZ privacy regulations.

Key Risks of Submitting Sensitive Data to GenAI Platforms

- Loss of Confidentiality & Privacy Breaches: Data entered into GenAI tools is often stored by the provider and could be accessed or disclosed in ways you don't intend. The NZ Privacy Commissioner warns that personal or confidential information entered into a generative AI may be retained by the provider and even used to train the model. This creates a risk that sensitive customer data or business secrets could later surface in AI outputs to other users. In short, once you paste proprietary text or personal data into an external AI service, you effectively lose exclusive control over that information's confidentiality. If that data includes personal information, it may constitute an unauthorised disclosure – a potential privacy breach under NZ's Privacy Act 2020.
- Data Retention and Training Data Exposure: Most GenAI providers (by default) use user inputs as part of ongoing model training. For example, OpenAI has stated it uses ChatGPT queries as training data to improve its models. This means any sensitive data your staff input could become embedded in the AI's knowledge base. Researchers have demonstrated that AI models can sometimes regurgitate pieces of their training data when prompted in certain ways. Thus, proprietary information accidentally submitted might later reappear in another user's query results. Even if direct output leakage is mitigated, the AI provider's employees or contractors may review stored prompts, or the data could be included in future versions of the model. This training data exposure risk was highlighted when Samsung discovered engineers had pasted secret source code and meeting notes into ChatGPT; the company swiftly banned GenAI use after realising that data could be absorbed into the public model.
- Platform Security & Data Breach Risks: Relying on external GenAI platforms means trusting that provider's security. If the platform is compromised or bugs occur, your submitted data could leak. In one incident, a ChatGPT glitch allowed users to see parts of other users' conversation histories (including titles containing sensitive info). The UK's National Cyber Security Centre (NCSC) notes that even if GenAI outputs are not directly shared between users, all queries are stored on the provider's servers, where they "will almost certainly be used for developing the LLM" – and those stored queries could be hacked, leaked, or accidentally made public.
- Regulatory and Compliance Implications: Any accidental disclosure of personal information to an unauthorised party (in this case, a GenAI provider and potentially its model) can trigger New Zealand's privacy breach notification requirements. The Privacy Act 2020 is technology-neutral – if the breach is likely to cause serious harm to an individual, the organisation must notify the Office of the Privacy Commissioner and affected individuals as soon as practicable. Beyond privacy law, consider confidentiality agreements or industry-specific rules: e.g. client contracts, NDA obligations, or financial and health data regulations.

Response Strategies for Accidental GenAI Data Exposure

Despite best efforts, mistakes happen. How organisations respond in the first hours can greatly affect damage control and compliance outcomes. Treat an accidental GenAI disclosure as you would a serious security incident or data breach. Key response steps include:

- Contain and Halt Further Exposure: Immediately instruct the individual to stop using the GenAI platform for any sensitive material. If the platform allows deletion of the submitted prompt or data, have them delete it (though this may not fully remove it from the provider's servers). Containment also means revoking any broader access if needed – e.g. temporarily blocking corporate access to the GenAI service until the incident is assessed. As with any data breach, quickly limiting additional data leakage is paramount. Identify exactly what information was disclosed and ensure no one else repeats the mistake while the incident is active.
- Preserve Information & Assess Impact: Record the details of what happened – which GenAI platform, what data was input, when, and by whom. This log will be useful for assessment and any notifications. Next, assess the sensitivity of the leaked data and potential impact. Was personal information involved (customer data, employee records)? How sensitive is the proprietary material (source code, financials, strategic plans)? Determine who could be harmed or what advantage could be gained if the data were exposed via the AI. Remember that information given to an AI might be incorporated into its training data and inform outputs to other users, so consider worst-case scenarios (e.g. a competitor querying the AI and uncovering hints of your Intellectual Property). Engage your privacy officer or data protection team to evaluate the seriousness.
- Engage Legal and Notify Authorities if Required: Loop in your legal counsel early. They will help determine legal obligations and guide communications. If you determine that a notifiable privacy breach has occurred, New Zealand's Privacy Act mandates notifying the Privacy Commissioner and the affected individuals "as soon as practicable" when a breach could cause serious harm. The Office of the Privacy Commissioner (OPC) expects notification within 72 hours of

becoming aware of such a breach. Work with legal/privacy teams to prepare a breach notification via the OPC's NotifyUs tool if needed, and draft clear communication for any affected parties explaining what happened and what is being done. Even if the leaked data is not personal (say it's proprietary business info), legal counsel can advise on whether other disclosures are warranted – for instance, informing an impacted business partner, or in rare cases, making a public statement if the incident could materially affect shareholders or customers. A frank discussion with the GenAI provider may be worthwhile—while you can't easily "un-train" the AI, some providers may delete submitted data from logs, especially for enterprise clients. In any case, ensure you comply with all regulatory reporting timelines and documentation.

- Inform key internal stakeholders and share the response plan. Transparency supports governance and helps allocate resources. Consider pausing GenAI use organisation-wide if a policy gap is revealed. Remind staff of data handling rules. For significant incidents, consider a formal investigation to identify the root cause (e.g. lack of awareness or deadline pressure). Focus on damage control and reassuring leadership—and possibly clients—that the situation is contained.
- Post-Incident Review and Prevention Update: Once the immediate crisis is handled, conduct a post-incident review. Analyse how and why the lapse occurred and what controls failed. Was there a lack of awareness or training? Was the policy not clear or enforced? Use these findings to strengthen your safeguards. Update your GenAI usage policies or data classification rules if necessary. You might decide to tighten technical controls (for example, deploying stricter Data Loss Prevention rules to block copying of certain data to web applications). This is also the stage to revisit your incident response plan: was the response timely and effective? A robust, tested incident response plan is crucial; it can prevent an incident from "becoming serious because of an unprepared response".

Preventative Measures to Mitigate GenAI Data Leakage Risk

The best way to manage GenAI data leaks is to prevent them. Establish a strong governance framework around the use of generative AI, combining policy, education, and technical controls. Key preventative measures include:

- Clear GenAI Usage Policies and Data Classification: Develop and enforce a GenAI Acceptable Use Policy. This policy should explicitly define what staff are not allowed to input into any AI service. For example, make it clear that any data classified as Confidential or Restricted (customer PII, financial records, intellectual property, etc.) must never be entered into public AI tools. Identify which business units (if any) are authorised to experiment with GenAI and under what conditions. Policies should also cover whether employees may use personal accounts or only corporate-approved AI accounts, and whether additional approvals are needed for certain use cases. Tie these rules into your existing data classification scheme – e.g., "Company Confidential" data cannot be shared with any third-party system without approval. By codifying this, you give employees a clear guideline and create a basis for enforcement or disciplinary action if violated.
- Staff Training and Awareness: Policy alone isn't enough; staff need to understand why it matters. Conduct regular training on the risks of GenAI and the contents of your GenAI usage policy. Use real examples to make it concrete: for instance, explain how an engineer uploading source code to get coding help could leak trade secrets, or how inputting a client's data could breach privacy laws. Emphasise that GenAI queries are not private – they are stored and reviewed by providers and potentially used in training. Training should also cover social engineering risks (e.g. adversaries creating fake "AI assistant" websites to phish data) and reinforce basic cyber hygiene when using new tools. The goal is to build a culture where employees think before they paste. Encourage a mindset that treating AI like a public forum is the safest default. Staff should also know the procedure to report any accidental disclosure immediately, without fear – a blameless reporting culture can lead to faster containment.
- Technical Controls and Monitoring: Back up your policies with technical measures. Many organisations deploy Data Loss Prevention (DLP) solutions and web filtering to curb risky behaviour. For example, a DLP system can detect patterns of sensitive data (like customer account numbers or code) being copied to web forms and block or alert on it. Similarly, you might configure network controls to restrict access to GenAI sites unless via approved methods. Some companies have opted to ban external AI tools until they can implement secure alternatives. If outright bans are not feasible, consider providing a sanctioned, secure GenAI solution – for instance, using an enterprise version of a GenAI platform that offers data isolation (no training on your inputs) and contractual privacy assurances. Major cloud providers now offer such enterprise LLM services where your prompts aren't shared in the global model. Additionally, implement monitoring for GenAI usage: your Security Information and Event Management (SIEM) or CASB (Cloud Access Security Broker) tools may detect unusual spikes in data going to AI services. Continuous monitoring with automated alerts can catch policy violations or suspicious usage early. Finally, ensure your incident response capability is up to date: prepare for the scenario of an AI-related data leak. Having a tested plan, as noted, will let you respond "quickly and effectively" if prevention fails.
- Governance and Compliance Measures: Treat GenAI use as high-risk and subject to oversight. The NZ Privacy Commissioner recommends senior leadership approval and thorough risk assessment before adoption. Executives should sign off on business use, balancing benefits with privacy and security risks. Conduct Privacy Impact and Algorithmic Impact Assessments to identify data exposure points and necessary controls. Align with frameworks like NIST's AI Risk Management Framework and its 2024 Generative AI Profile, which help manage GenAI-specific risks. Follow standards such as ISO/IEC 27001, 27701, and the new ISO/IEC 42001 for AI governance and data protection. Ensure compliance with NZ's Privacy Act and sector-specific rules—verify data storage, usage, and address these in vendor due diligence and contracts. Integrate GenAI oversight into your risk governance, update the board on AI risks, and report regularly on policy compliance.

Accidental leaks of sensitive data into generative AI platforms are a 21st-century twist on the classic insider mistake. They blend human error with cutting-edge technology – and the stakes can be high. For New Zealand organisations, the message is clear: preventing and managing GenAI-related data breaches must be part of your cybersecurity and privacy strategy. Organisations have a duty to establish prudent controls (policies, training, technical safeguards) so that innovation with AI does not outpace governance.

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: