NZ Incident Response Bulletin

Standard Edition – July 2026 – Issue #90

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

'Five Eyes' intelligence alliance warns that new AI models pose urgent cyber risk

Five Eyes cybersecurity agencies have warned that advanced artificial intelligence models could significantly increase the speed, scale, and sophistication of cyberattacks within months. The warning highlights that AI may help attackers identify vulnerabilities, develop working exploits, and conduct larger-scale operations with less specialist expertise. For executives, the issue is no longer a future technology concern or a matter for security teams alone. AI-enabled cyber risk has direct implications for business continuity, operational resilience, market confidence, and long-term value. Organisations should expect the time between vulnerability disclosure and exploitation to continue shrinking. Leadership priorities should include faster patching, reduced exposure of internet-facing systems, stronger identity controls, tested incident-response arrangements, and clear executive accountability for cyber risk. While AI can also strengthen cyber defence, this will depend on whether organisations adopt, govern, and use these capabilities effectively.

NZSIS warns Kiwis about targeting by Chinese spies over job, networking sites

New Zealand's intelligence service has warned that Chinese military intelligence personnel are using professional networking platforms and online job sites to identify and approach people with access to sensitive information. The activity reportedly involves intelligence officers posing as recruiters or consultants representing convincing but fictitious companies. Initial requests may appear harmless, such as producing research or commentary, but can progress towards military, political or government information that is not publicly available. Security-clearance holders, defence personnel and government employees are considered particularly exposed, although contractors, advisers and former employees may also possess valuable information. For executives, the story highlights the convergence of cyber-enabled social engineering, insider risk and foreign espionage. Organisations handling sensitive information should review what personnel disclose through LinkedIn and similar services, establish processes for reporting suspicious approaches and extend security awareness beyond conventional phishing emails. Employment history, project descriptions, clearance information and professional connections can collectively help an adversary identify, profile and manipulate a valuable target.

New cutting edge AI models limited to Trump-approved customers

OpenAI temporarily limited early access to GPT-5.6 Sol while the United States Government assessed the model's national-security and cybersecurity risks. The model's advanced capabilities include identifying and helping remediate software vulnerabilities, although OpenAI acknowledged that unforeseen risks could arise when it is combined with other tools. Access was initially limited to a small group of approved customers as part of a phased release. OpenAI subsequently made the GPT-5.6 model family generally available on 9 July 2026 following the limited preview and additional security testing.

Australia

Australian Clinical Labs says limited data taken in SunDoctors cyberattack

Australian Clinical Labs has confirmed that a cyberattack affecting an external IT provider used by its SunDoctors business resulted in unauthorised access to part of its systems and the theft of some data. Most of the affected information consisted of basic contact details and limited health information relating mainly to skin cancer checks and testing. The company said there was no evidence that the stolen information had been published online. Because investigators could not determine exactly which individuals were affected, SunDoctors notified approximately 280,000 people whose information may have been accessed. Australian Clinical Labs said the incident was limited to SunDoctors and did not affect its broader pathology or laboratory operations.

ASD to retire Essential Eight cyber security framework within next two years

The Australian Signals Directorate plans to retire its Essential Eight cybersecurity framework within two years and replace it with a broader "Essentials" series. The updated guidance is intended to reflect modern technology environments, including cloud services, operational technology, enterprise systems and potentially agentic artificial intelligence. The Essential Eight was originally designed primarily for traditional on-premises IT and does not always align effectively with cloud and software-as-a-service environments, where security responsibilities are shared with providers. Both frameworks are expected to operate during a transition period, with deprecation of the Essential Eight likely to begin after about 12 months. Organisations currently using the framework should continue their existing security programmes while preparing to map their controls, assessments and reporting to the new outcome-focused guidance.

World

US shortens cyber fix window to three days as AI threats rise

CISA has introduced a risk-based vulnerability-remediation process for United States Federal Civilian Executive Branch agencies. Under Binding Operational Directive 26-04, vulnerabilities assessed as presenting the highest risk must be remediated within three days. Other vulnerabilities receive longer remediation timelines or may be addressed during a scheduled system upgrade, depending on factors such as active exploitation, system exposure and potential impact. Although the directive does not apply directly to New Zealand organisations, it provides a useful model for prioritising remediation according to operational risk rather than severity scores alone.

Hacking group claims major hack of Novo Nordisk and attempted $25 million extortion

Novo Nordisk confirmed unauthorised access to limited internal systems after the FulcrumSec extortion group claimed it had stolen more than 1.3 terabytes of data and demanded US$25 million. The alleged material included source code, clinical-trial information, unreleased product details and personal data, although the company did not confirm the scale of the attackers' claims. Operations continued. The incident highlights how cyberattacks on pharmaceutical companies can threaten intellectual property, regulatory activity, commercial strategy and public trust, not only personal information.

India's Tata Electronics hit by cyber breach claiming to expose Apple, Tesla trade secrets

Tata Electronics confirmed a cyber incident after the World Leaks ransomware group published more than 200,000 files, totalling over 630 gigabytes, on the dark web. The exposed material reportedly included manufacturing specifications, component designs, emails, event logs and employee passport copies, with some documents linked to customers Apple and Tesla. Although Tata said operations were unaffected, the breach highlights how attacks on suppliers can expose valuable intellectual property and confidential information belonging to multiple organisations. It also shows that uninterrupted operations do not necessarily mean the consequences of a cyberattack are limited.

France's statistics department reports cyberattack on staff data

A cyberattack on France's national statistics institute, Insee, exposed professional directory information for about 12,800 current and former staff and associated civil-service personnel. The compromised data included names and work contact details, but not passwords, banking information, health records, social-security numbers or personal contact information. While the breach was limited, the information could still support targeted phishing, impersonation and intelligence-gathering. Organisations should warn affected staff, monitor for follow-on attacks, strengthen identity verification and review whether internal directories contain more information than necessary.

Hackers trick Meta AI support bot to infiltrate Obama White House Instagram account

Hackers exploited weaknesses in Meta's AI-powered customer-support system to take control of prominent Instagram accounts, including Barack Obama's former White House account, Sephora and a senior US Space Force official. Demonstrations circulated online showing attackers persuading the chatbot to associate a targeted account with a new email address. After receiving a verification code at that address, the attacker could reset the account password. Virtual private networks were reportedly used in some cases to imitate the account owner's location and evade safeguards. Meta said the vulnerability had been resolved and that it was securing affected accounts, although the total number of victims was unclear. The incident demonstrates a significant risk associated with allowing AI support tools to perform security-sensitive actions. An attacker may not need to defeat a conventional authentication system when they can manipulate the automated process responsible for account recovery.

Spyware firm targeted WhatsApp users in defiance of US court order, Meta says

WhatsApp disrupted spear-phishing attacks linked to NSO Group that targeted users in Jordan and Lebanon through malicious links. Meta said the activity may have breached a US court order restricting NSO's use of WhatsApp following litigation over Pegasus spyware. The incident shows that end-to-end encryption cannot fully protect users when spyware compromises the device itself, allowing attackers to access messages before encryption or after they are displayed. It also highlights the difficulty of controlling commercial surveillance technology once it has been developed and distributed.

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.

18/06/2026 - Reported widespread credential exposure affecting Fortinet Firewalls and VPN Gateways

Our Views:

38th Annual FIRST Conference

Key Takeaway: Our attendance at FIRSTCON26 confirmed that New Zealand is tracking well against international incident response practices. Organisations are adopting current technologies, adapting to emerging threats, and placing greater emphasis on cyber resilience. However, preparedness must continue to evolve as artificial intelligence, identity-based attacks, and cloud environments shift the frontline reality of cyber incidents.

The 38th Annual FIRST Conference was held in Denver in June and brought together approximately 700 cybersecurity professionals from around the world. The conference provided a vital opportunity for incident responders, researchers, government agencies, and cybersecurity leaders to share practical experiences and strengthen trusted international relationships. These cross-border relationships are increasingly critical. A single modern cyber event may involve a cloud provider in one country, infrastructure hosted in another, affected customers across several jurisdictions, and a threat actor operating from elsewhere. Effective response depends not only on technical capability, but on timely information sharing and access to trusted global contacts.

The Dual-Edged Sword of AI in Incident Response

A consistent theme throughout the conference was the growing use of artificial intelligence (AI) by both threat actors and incident defenders.

- The Threat: AI is allowing threat actors to automate reconnaissance, identify vulnerabilities faster, develop highly convincing phishing content, and increase the speed and scale of attacks.
- The Defence: Conversely, defenders are leveraging AI to analyse massive volumes of log data, identify malicious patterns, summarise technical evidence, and accelerate investigative workflows.

While these defensive capabilities offer clear benefits, they do not remove the need for experienced human judgement. AI-generated findings must still be verified against underlying forensic evidence - particularly when conclusions support regulatory reporting, legal proceedings, insurance claims, or public communications. Organisations adopting AI-enabled forensic tools must carefully consider how evidence is collected, where data is processed, and whether findings can be independently reproduced.

Shifting Frontiers: Identity and Cloud Evidence

The conference reinforced a clear shift in attacker behaviour: threat actors are increasingly targeting user accounts, session tokens, authentication processes, and administrative workflows rather than relying solely on traditional malware. Once an attacker obtains valid credentials, their activity initially mirrors that of a legitimate user. This fundamentally changes the nature of a forensic investigation. To respond effectively, organisations require immediate access to cloud audit records, authentication logs, privileged access events, endpoint data, and third-party service logs. Without this evidence, determining how an attacker gained access, what information was compromised, and whether the incident has been fully contained becomes exceptionally difficult.

The Vulnerability Bottleneck

FIRST forecasts approximately 66,000 CVE disclosures in 2026. The increase reflects a combination of AI-assisted vulnerability discovery and structural changes in the vulnerability ecosystem, including expanded advisory curation, retrospective CVE assignment and reporting backlogs. However, the number showing strong indicators of near-term exploitation remains comparatively stable, reinforcing the need for risk-based prioritisation.

The Frontline Reality for New Zealand Organisations

Based on our discussions and observations at FIRSTCON26, we know that New Zealand organisations that are mature in their IR program align with current international incident-response practices. Many are actively improving visibility across cloud and identity systems, updating incident response plans, and testing their preparedness through simulations. However, alignment should provide confidence, not complacency. Technology alone does not equal readiness. A security platform has limited value if it is improperly configured, or if an incident response plan is executed by a team that has never practised responding under pressure. To ensure your preparedness is demonstrated through operational reality rather than policy alone, organisations should actively review the following areas:

- Log Retention & Accessibility: Confirm that critical cloud, identity, and authentication logs are retained for an adequate duration and can be exported in a usable format during a crisis.
- Vulnerability Governance: Move away from blanket patching cycles and implement risk-based prioritisation that factors in your specific business context.
- Executive Exercises: Test incident response arrangements not just with IT, but through tabletop simulations involving executives, legal advisers, and communications teams.
- Evidence-Based Assurance: Ensure you can actively demonstrate that controls are operating, alerts are actively investigated, and backups can be successfully restored under pressure.

We welcome the opportunity to meet with clients to share further insights from FIRSTCON26 and discuss how these developments apply to your cybersecurity, forensic readiness, and incident response programmes.

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: