NZ Incident Response Bulletin

Standard Edition –May 2026 – Issue #88

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

Inland Revenue warns of rise in malicious activity as hackers access 300 myIR accounts

This report highlights a targeted attack against Inland Revenue's myIR platform in which cyber criminals successfully accessed about 300 accounts over a two-week period. Inland Revenue said it detected more than 500,000 malicious logon attempts during the month, suggesting a broad credential-based attack rather than a one-off incident. Importantly, the agency reported no financial losses, and said two-step verification prevented access to most accounts, including around 900 where the correct password had been entered but additional authentication blocked entry. The affected accounts were those without two-step verification enabled. Inland Revenue is contacting impacted users and has pointed to password reuse across less secure services as a likely cause. For executives, the significance is clear: identity systems remain highly vulnerable to credential stuffing, and basic controls such as unique passwords and multi-factor authentication continue to provide strong, measurable risk reduction when consistently adopted.

Fewer New Zealanders experienced harm from cyber attacks

The National Cyber Security Centre reported an encouraging reduction in the proportion of New Zealanders suffering harm from cyber incidents, with the figure dropping from 36% in 2024 to 27% in 2025 among those who experienced an online threat. The research suggests that awareness campaigns and improved user behaviour are starting to have an effect. In particular, use of two-factor authentication on main online accounts rose from 38% to 43%, and password manager adoption also increased. However, the release also shows that threat exposure remains widespread: 48% of adult New Zealanders said they had experienced an online threat in the previous six months, and only 56% reported it. Older New Zealanders were significantly less likely to report incidents, with apathy identified as a major barrier. For executives, this is a mixed but useful signal: baseline cyber hygiene appears to be improving, yet threat frequency remains high and under-reporting continues to limit visibility. That means organisations should not mistake improved resilience for reduced exposure.

Notes from the Asia-Pacific region: Cyber risk is outpacing organizational response

The article highlights growing concern that New Zealand organisations are not adapting quickly enough to the country's worsening cyber risk environment. Referencing a March 2026 address by New Zealand Privacy Commissioner Michael Webster, it notes that cybersecurity has shifted from a technical issue to a board-level governance priority, but many organisations still appear to be innovating faster than they are managing privacy and cyber risk. The article points to serious privacy breach data showing that 61% of serious privacy breaches are now linked to malicious activity, with unauthorised access and inappropriate employee browsing becoming more prominent concerns. A key message is that cybersecurity and privacy can no longer operate separately. Privacy outcomes depend on effective security safeguards, while security decisions increasingly carry privacy consequences. For executives, the takeaway is clear: organisations need stronger integration between cyber, privacy, governance, culture, access controls, and risk management to protect personal information effectively.

Microsoft announces boost in NZ AI training

Microsoft will expand its AI and digital skills programme in New Zealand, aiming to provide training access to another 200,000 people by the end of 2028. The initiative supports New Zealand's broader AI strategy and reflects growing demand for practical AI capability across business, education, government, and community sectors. For executives, the key takeaway is that AI adoption is not only a technology investment, but a workforce readiness issue requiring training, governance, security, and responsible use practices.

Australia

Booking.com warns customers of possible data and security breach by 'unauthorised parties'

This article is relevant to Australian executives because it highlights how a breach at a major digital platform can quickly create local scam and consumer-protection risks. Booking.com warned some customers that contact details may have been accessed, increasing the risk of credible phishing, fake payment requests and accommodation-related impersonation scams. For executives, the key lesson is that third-party incidents can create downstream exposure for customers, staff and brands, even when their organisation is not directly breached.

Accused hacker allegedly targeted government departments, courthouse and gym, court hears

This ABC report shows how cyber disruption can come from individual actors, not only organised crime or nation-state groups. Prosecutors alleged an Adelaide man targeted multiple organisations, including government departments and a courthouse, causing staff to lose email access for a day. The case highlights that even attention-seeking cyber activity can disrupt essential operations. Organisations should maintain strong identity controls, logging, access management and incident response capability across critical systems and shared infrastructure.

Your identity could be sold for as little as $200 on the dark web, experts warn

Stolen Australian identity data is being sold on dark web marketplaces, with a complete identity reportedly available for as little as $200. Around 1.1 million Australian accounts were leaked in early 2026, exposing individuals to fraud, account takeover and identity theft. Criminals can buy payment details, passport scans, email accounts, corporate credentials and social media profiles. Consumers should use unique passwords, enable multi-factor authentication, monitor accounts and watch for suspicious activity.

'Almost foolproof': Why phishing scams targeting travellers are so dangerous

Travel-related data breaches are increasing the risk of highly personalised phishing scams targeting Australian travellers. Exposed details, such as names, contact information, travel dates and bookings, can help criminals create convincing messages that appear to come from legitimate providers. Attackers may use urgent payment requests, refund offers or verification links to steal money or banking details. Travellers should avoid clicking unsolicited links, use official booking platforms and verify unexpected requests directly with providers.

World

Germany intelligence agency warns of Russian APT28 cyber spying

Germany's warning about APT28 highlights the continued threat of state-linked cyber espionage against governments and critical sectors. Reuters reported that the Russian-linked group exploited vulnerable TP-Link routers to target military, government and critical infrastructure organisations, with several thousand routers targeted globally. The case shows how ordinary internet-facing devices can be used as access points for sophisticated espionage. Organisations with distributed edge devices, unmanaged branch technology or weak patching should treat low-cost infrastructure as a potential strategic exposure point.

UK cyber agency handling four major incidents a week as nation-state attacks surge

The UK's National Cyber Security Centre warned that Britain is handling around four nationally significant cyber incidents each week, with the most serious attacks increasingly linked to hostile states. The article highlights a shift from isolated criminal activity to more frequent and consequential state-backed threats involving countries such as China, Iran and Russia. Organisations outside government and defence may still be exposed to geopolitically motivated cyber activity, making scenario planning, crisis readiness and coordination between cyber security, risk, legal and communications teams increasingly important.

Cyberattack at French identity document agency may have exposed personal data

A cyberattack on France's National Agency for Secure Documents may have exposed personal data linked to passports, identity cards, residence permits and driver's licences. The incident shows how attacks on national identity systems can quickly become trust, fraud and governance issues, not just technical failures. Centralised identity platforms hold highly sensitive data, making them attractive targets with significant consequences if breached. Organisations managing large customer or citizen datasets should ensure strong security architecture, breach response capability and clear communications planning.

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.

24/04/2026 – FIRESTARTER Malware affecting Cisco ASA and FTD

Our Views:

Cyber Simulations and Tabletop Exercises

Cyber simulation exercises, in particular tabletop and gold team exercises, involving executives and senior decision-makers, are one of the most effective ways for New Zealand organisations to improve cyber resilience.

The New Zealand National Cyber Security Centre (NCSC) has repeatedly highlighted the importance of exercising incident response plans, noting that regular testing helps ensure organisations know "what to do in the event of a cyber incident." Increasingly, regulators, insurers, auditors and boards are also expecting organisations to demonstrate not just that plans exist, but that they have been tested in realistic conditions.

A well-run tabletop exercise places organisational teams into a simulated cyber crisis. Participants are forced to make decisions with incomplete information, conflicting priorities and escalating operational impacts. In many cases, the technical compromise itself becomes secondary to the broader organisational challenges that emerge such as media scrutiny, legal obligations, customer communications, operational continuity, third-party dependencies and reputational risk.

For organisations undertaking these exercises for the first time, the findings can be enlightening. Teams often discover that escalation pathways are unclear, roles overlap, or key decisions have never been discussed in advance. It is common to identify uncertainty around who manages and authorises customer notifications, who engages regulators, whether extortion demands or ransom payments would ever be considered, or how business continuity processes will operate if core systems are unavailable. A cyber simulation creates a controlled environment where organisations can safely expose weaknesses before a real incident does. Even relatively short tabletop exercises frequently reveal significant gaps in communication, governance and operational readiness.

However, after working with some of our clients for several years, we have found that the most significant benefits are seen in organisations that repeat these exercises year after year. We have seen how ongoing simulation programmes fundamentally improve organisational maturity and help normalise cyber incidents as executive-level business risks rather than purely IT problems.

When a real incident occurs, we see that teams who have repeatedly practised incident response scenarios are noticeably calmer and more structured in their response. They understand escalation thresholds. They know who needs to be involved. They understand how information flows during a crisis. Most importantly, they are less likely to lose valuable time debating basic process questions during the early stages of an incident. Mature organisations also treat simulation findings as formal improvement actions, tracking remediation activities over time and measuring whether identified weaknesses are being reduced between exercises.

Many organisations begin with highly facilitated tabletop workshops where participants sit together in a single room and work collaboratively through a scenario with guidance from facilitators. These exercises are intentionally supportive and educational in nature, helping participants understand incident response processes, clarify responsibilities and become familiar with the pressures associated with a cyber event. For organisations undertaking their first simulation or who have new team members, this approach is often the most effective way to build confidence and establish baseline capability.

However, as organisations repeat exercises and their maturity develops, we have seen a noticeable recent shift toward a demand for far more realistic and operationally demanding simulations. Increasingly, our more experienced clients are requesting complex scenarios designed to deliberately stress test decision-making, communication pathways and escalation processes under pressure.

These advanced simulations involve multiple concurrent response streams operating in separate "war rooms", including technical response teams, executive management groups and board-level participants, each receiving different pieces of information at different times throughout the exercise. This design better replicates the fragmented, high-pressure and fast-moving operating environment commonly experienced during real cyber incidents, where technical responders may have incomplete forensic visibility, executives are dealing with operational and reputational consequences, and boards are receiving strategic risk updates independently.

The result is a far more immersive and realistic exercise environment that tests not only technical response capability, but also organisational coordination, leadership communication, decision authority and crisis governance maturity.

Our more experienced simulation clients demonstrate how cyber resilience is built through repetition, refinement and realistic practice. With repeated exercises we see a shift from reactive behaviour toward coordinated decision-making. Discussions become faster, terminology becomes standardised, and teams develop greater confidence operating under pressure and ambiguity.

Over the last year we have seen a positive shift in the cyber simulation exercise landscape with more organisations willing to learn, grow and stress test their processes in a safe space. We continue to believe that consistently undertaking simulation exercises year after year and growing this capacity through increasingly realistic scenarios will ensure organisations respond more effectively when a real crisis eventually occurs.

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: