NZ Incident Response Bulletin

Standard Edition – September 2025 – Issue #80

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 NZ SMEs have experienced cyber threats, says NCSC

A recent survey by New Zealand's National Cyber Security Centre (NCSC) has revealed that over half of small and medium-sized enterprises (SMEs) in the country have encountered cyber threats. Despite this, a significant number of SMEs remain underprepared, with limited investment in cybersecurity measures. The report highlights a worrying trend: while many businesses are aware of the growing cyber threat landscape, few are taking adequate steps to address their vulnerabilities. Most incidents involved phishing attacks, malware, and unauthorised access attempts. The NCSC emphasises the need for SMEs to adopt basic security practices such as multi-factor authentication, regular software updates, and employee training. The centre also warns that cybercriminals are increasingly targeting smaller organisations due to their often weaker defences. As cyber risks continue to evolve, the NCSC urges SMEs to shift from reactive to proactive security strategies to protect sensitive data and maintain operational resilience.

New Zealand joins international partners in countering China-linked cyber attacks

New Zealand has formally joined international partners, including the United States and United Kingdom, in attributing a series of malicious cyber activities to a China-linked threat actor known as APT40. The coordinated response follows detailed intelligence assessments indicating that APT40, associated with China's Ministry of State Security, has conducted widespread cyber intrusions targeting government agencies, critical infrastructure, and private sector entities. New Zealand's Government Communications Security Bureau (GCSB) confirmed that local networks had been scanned by the group, though no significant breaches were reported. The move signals a shift in New Zealand's cybersecurity posture, aligning more directly with global allies in calling out state-sponsored cyber threats. The Minister for the Intelligence Services, Judith Collins, emphasised the importance of defending democratic institutions from such threats and enhancing international cooperation. The announcement reflects growing geopolitical tensions in cyberspace and the increasing importance of attribution and deterrence in national cybersecurity strategies.

World

Ransomware, data theft strike telecoms in UK and Australia, raising concerns for critical infrastructure

Telecoms companies in both the UK and Australia have recently suffered serious cyber incidents, underlining rising risks to critical infrastructure. In the UK, Colt—a major telecom operator—was attacked by the Warlock ransomware gang. The breach hit several business support systems, prompting the company to take some services offline pre-emptively. While customer-facing infrastructure was reportedly not directly compromised, internal systems remain in recovery mode. Colt has notified relevant authorities and is engaging third-party security experts.

Simultaneously in Australia, iiNet (part of the TPG group) experienced unauthorized access to its order management system via compromised employee credentials. The breach affected about 280,000 people, exposing ~10,000 phone numbers and addresses and 1,700 modem passwords. Importantly, sensitive documents like identity docs or banking details were not stolen. iiNet activated its incident-response plan, contacted affected customers, and engaged external cybersecurity and regulatory bodies.

These incidents highlight that telecoms—deemed critical infrastructure—are high-value targets for attackers, especially via third-party risks and credential compromise. They stress the need for organisations in this sector to have robust detection of data exfiltration, strong access controls (e.g. strong / unique passwords, multi-factor authentication), real-time monitoring, and rapid coordination with regulators and cyber-experts when breaches occur.

Australian Information Commissioner takes civil penalty action against Optus

The Office of the Australian Information Commissioner (OAIC) has initiated civil penalty proceedings against Optus over the massive 2022 data breach that compromised the personal information of over 10 million Australians. The OAIC alleges that Optus failed to take reasonable steps to protect customer data, in breach of the Privacy Act. Specifically, the Commissioner argues that Optus retained personal information for longer than necessary and did not adequately secure it, exposing individuals to serious risk of harm. This legal action marks a significant enforcement move and reflects the growing regulatory pressure on companies to uphold data protection obligations. If the Federal Court finds against Optus, it could face substantial financial penalties and be required to improve its data governance practices. The case underscores the importance of proactive data lifecycle management, transparent breach reporting, and alignment with privacy law requirements—particularly in an era of increasing cyber threats and heightened public scrutiny.

African authorities dismantle massive cybercrime and fraud networks, recover millions

In a major international law enforcement operation, African authorities, in collaboration with INTERPOL, have dismantled extensive cybercrime and fraud networks operating across 25 countries. The operation, named Africa Cyber Surge III, led to the arrest of 14 suspected cybercriminals and the identification of over 20,000 suspicious cyber networks. These networks were linked to a range of illicit activities, including phishing, business email compromise (BEC), online scams, and financial fraud. Authorities were able to seize nearly USD 3 million in illicitly obtained assets and freeze dozens of bank accounts tied to criminal operations.

The operation also involved the takedown of malicious infrastructure, including websites and command-and-control servers used in cyber attacks. INTERPOL emphasised that many of the cybercriminals exploited vulnerabilities in financial institutions and small businesses, highlighting the need for enhanced cybersecurity across both public and private sectors. The initiative underscores the importance of regional and international cooperation in tackling transnational cyber threats and reinforces calls for stronger digital resilience frameworks across Africa. It also reflects a growing capacity among African law enforcement agencies to address increasingly sophisticated cyber threats with support from global partners.

Australia's TPG Telecom flags cyber incident in its iiNet system

TPG Telecom, one of Australia's largest telecommunications providers, has reported a cyber incident involving its iiNet subsidiary. The breach affected a legacy system used for managing customer orders, resulting in unauthorised access to the data of approximately 280,000 customers. TPG disclosed that roughly 10,000 customer addresses and contact numbers, along with 1,700 modem passwords, were accessed by attackers. The exposed data did not include identification documents or financial information.

The incident was discovered on August 14, and TPG took immediate steps to secure the system, notify regulators, and begin contacting affected customers. An external cybersecurity firm has been engaged to investigate the breach. TPG stressed that the impacted system was old and isolated from core operations, with no evidence suggesting broader network compromise.

This incident underscores the persistent vulnerabilities associated with legacy IT infrastructure and highlights the importance of regular system audits and decommissioning of outdated platforms. It also signals ongoing threats to the telecom sector, reinforcing the need for enhanced credential security, timely breach detection, and comprehensive incident response strategies. As regulators continue to scrutinise cybersecurity performance, organisations are under pressure to modernise defences and improve transparency around cyber risk and data protection practices.

ANZ reports drop in scam losses as customers embrace new protections

Between October 2024 and June 2025, ANZ observed a 15% drop in financial losses due to scam activity compared to the previous year. This reduction builds on a larger 49% reduction ANZ had reported in the prior reporting period. The bank attributes the improvements to a multi-layered strategy that includes new security tools, greater customer uptake of security features, and enhanced educational efforts. One new feature is "Digital Padlock," a capability designed as a kill-switch or last-resort lock for accounts to protect customers from unauthorised transactions. These results suggest that combining technology, customer behaviour change, and awareness can produce measurable gains in curbing scam-related losses.

Australian banking regulator warns geopolitical tensions could lead to more cyber attacks

On August 20, 2025, the Australian Prudential Regulation Authority (APRA) issued a warning that rising geopolitical tensions increase the risk landscape for Australia's financial sector. APRA said that its oversight will be stepped up, and that it expects banks to intensify their cyber risk planning and stress testing in light of possible cross-border, state-sponsored, or politically motivated attacks. While this is still in the cautionary stage (not tied to any specific new breach), it reflects the increasing awareness that cyber risk is not just technical or financial, but strategic, linked to broader global tensions.

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.

28/08/2025 – China state-sponsored actors target networks globally

Our Views:

Beyond Passwords & MFA: Why Device Filtering Matters

Strong passwords and Multi-Factor Authentication (MFA) are now considered the bare minimum for protecting organisational systems. These controls stop many attacks — but they don't stop them all. In fact, attackers are increasingly shifting their focus away from simply stealing credentials and towards exploiting the devices people use to log in. A personal laptop that is missing critical security patches, a contractor's phone without encryption, or an old desktop that hasn't been properly registered can all become back doors into corporate systems. Even if the person logs in with MFA, the underlying device may already be compromised, leaving the organisation exposed. Device filtering addresses this risk by going beyond the "who" and adding the "what" — ensuring that only trusted, well-managed, and secure devices can access sensitive systems.

Breaches That Could Have Been Stopped

Breach 1: An Employee with a Malware-Infected Laptop

We have seen examples where accounts have been permitted access from computer makes and models that the company does not supply. A firm can suffer a data breach if an employee logs into corporate email from such an unmanaged personal device. Even though the employee may use MFA to log in, the compromised laptop can capture the session token. Attackers then bypass MFA and gain access to sensitive information.

Breach 2: A Threat Actor Logging In with Stolen MFA Credentials

In another scenario, a threat actor successfully phishes an employee, stealing both their username and MFA credentials. Instead of using the employee's device, the attacker attempts to log in from their own machine. Without device filtering, this activity may appear legitimate, as the credentials and MFA check both succeed. Device filtering, however, would spot that the login is coming from an unrecognised and non-compliant device. Access could then be blocked, or restricted to read-only, preventing the attacker from fully breaching the system.

What is Device Filtering?

Device filtering (sometimes called "context-aware access") means applying rules that decide:

- Should this device be allowed to access corporate data at all?
- Should access be limited to certain apps or functions if the device is personal or unmanaged?
- Should higher-risk devices have to meet extra requirements (e.g. re-authenticate, use stronger encryption, or be blocked altogether)?

Instead of a one-size-fits-all policy, device filtering allows organisations to tailor access based on real-world risk.

How the Big Players Do It?

Microsoft:

Microsoft's identity platform lets organisations include or exclude devices from access policies based on their type, ownership (work vs personal), or how they were set up. This means company-owned laptops can get full access, while personal or unregistered devices can be restricted or required to pass extra checks.

Google:

Google offers "Context-Aware Access," where managers can set rules such as: only allow access to Drive or Gmail from devices that are encrypted, updated to the latest version, and registered with the company. Contractors or unmanaged devices may be limited to web-only access or blocked from downloading files.

Both approaches give organisations far more flexibility than simply saying "yes" or "no" to a login attempt.

Key Governance Lessons & Recommendations

Keep policies clear and under control

Many organisations build up too many overlapping conditional access rules over time. This creates confusion about what is actually enforced and leaves space for mistakes. Simplify policies, give them clear names, and review them regularly to remove duplicates or outdated rules.

Tightly manage exceptions

Excluding certain accounts (like contractors, service accounts, or emergency "break-glass" accounts) may be necessary, but every exclusion creates a potential weak spot. Leaders should ensure all exceptions are documented, approved at the right level, and revisited frequently to avoid creeping risk.

Cover every type of user and device

Security rules must apply beyond employees. Guest accounts, third-party contractors, automated systems, and older applications often fall outside standard protections. Governance teams should confirm that these areas are included in access reviews and not left as blind spots.

Invest in proper device management

Device filtering only works if the organisation can clearly identify and manage the devices connecting to its systems. This means keeping an accurate register of company-owned devices, ensuring they are patched and encrypted, and deciding what level of access, if any, should be given to personal devices.

Monitor effectiveness and demand regular reporting

Boards and executives should ask for metrics that show how well policies are working — such as the number of blocked sign-ins from non-compliant devices, how many unmanaged devices are still in use, and how often emergency accounts are accessed. Regular reporting helps governance bodies confirm that access controls are effective and aligned with risk appetite.

The shift from identity-only security (passwords and MFA) to identity plus device trust is now essential. Device filtering ensures that only secure, well-managed devices can connect to your systems, reducing the risk of attackers slipping in through unmanaged endpoints. For non-technical leaders, the message is simple: it's no longer just about who logs in, but also about what they're logging in from.

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: