NZ Incident Response Bulletin

Standard Edition –January 2026 – Issue #84

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

Review commissioned of Manage My Health cyber security breach

The New Zealand Government has commissioned an independent review into the cyber security breach affecting the Manage My Health patient portal, following the exposure of sensitive personal and health information. Announced by the Minister of Health, the review will be led by Ministry of Health and will examine how the incident occurred, the adequacy of security controls in place, and the effectiveness of the incident response. The review will also assess governance and oversight arrangements for digital health services operated by third-party providers. The Minister emphasised that public trust in digital health systems is critical and that organisations handling health data—whether public or private—must meet high cyber security standards. The terms of reference will be developed in consultation with the National Cyber Security Centre and the Government Chief Digital Officer. Findings and recommendations will be used to strengthen protections across the wider health sector and reduce the risk of future breaches.

NZ cyber losses more than double amid email scams

In a Q3 2025 national cyber report, the National Cyber Security Centre revealed that direct financial losses from cybercrime more than doubled compared with the previous quarter, rising to NZ$12.4 million. The increase was primarily driven by business email compromise (BEC) campaigns and falsified payment directives that successfully duped organisations into sending funds to criminal accounts. Over 1,200 incidents were formally reported to the NCSC during this period, demonstrating broad awareness of malicious activity across sectors. High-value fraud cases disproportionately influenced the financial totals, indicating that attackers are increasingly targeting larger organisations or larger payment workflows. The report underscores that while traditional malware threats persist, *social engineering-driven financial fraud* remains one of the most damaging vectors for local entities. It signals a need for stronger transactional verification processes, enhanced staff education, and more widespread deployment of identity and email security controls across New Zealand businesses.

26,000 New Zealanders' devices infected with malicious software, cyber security agency warns

In December 2025, New Zealand's National Cyber Security Centre (NCSC) issued an unusually large direct alert to citizens after detecting that around 26,000 devices were likely compromised by Lumma Stealer malware. This malicious software is designed to harvest sensitive data such as email credentials and passwords, potentially putting victims at risk of follow-on attacks like account takeover and fraud. The NCSC proactively contacted affected individuals with remediation guidance and worked with financial institutions and government partners on protective measures. This scale of notification highlights the sophistication and pervasiveness of modern malware campaigns targeting private users' personal devices. The incident also underscores the importance of robust endpoint controls, credential hygiene, and rapid public-facing communication when large clusters of infections are identified.

BNZ concern over SMEs' attitude to cyber security as scams net thousands

BNZ warns that many small and medium-sized businesses (SMEs) remain underprepared for scams, even as threat activity rises. BNZ's survey found about half of SMEs were targeted by scams in the past year, with victims losing an average of roughly $5,000 per incident. Despite this, almost half of SMEs reported struggling to prioritise scam education and cyber training, and 45% did not view cyber education as a key priority, even though 64% said scam activity increased over the last 12 months. BNZ notes a gap between confidence and outcomes: while 53% of owners felt "prepared", nearly half of that group still engaged with a scam attempt. The most common tactics were "low-tech" social engineering, including cold calls seeking sensitive information (27%), bank impersonation (17%), and invoice scams with altered bank details (10%); ransomware was reported by only 2%. BNZ recommends practical controls like multi-factor authentication and dual approval for payments, alongside staff upskilling via trusted resources.

Australia

Cyber attacks that occurred this year and how you can protect your data

Australia's ABC reviews the cyber threat landscape across 2025, highlighting how breaches affected multiple sectors and why the true "biggest breach" may be one the public never hears about (because intrusions can be stealthy and disclosure isn't always timely). The article points to Australia's breach-reporting data (including the OAIC's Notifiable Data Breaches statistics dashboard) showing hundreds of reported breaches in the first half of the year, with a majority attributed to malicious or criminal activity. It then shifts to practical, executive-friendly guidance: reduce unnecessary data sharing, be wary of insecure channels (for example, unencrypted communications), and expect that once personal data is handed to a service provider, individual control is limited. For organisations, the emphasis is on governance and hygiene—strong privacy and security training, clear protocols, board-level attention to privacy risk, and limiting data retention to what's genuinely needed.

Australia leads world in costly, rising ransomware toll

A major industry research analysis published in early December 2025 found that Australian organisations reported the highest proportion of ransomware attacks globally in 2025, with nearly 35 % of cyberattacks involving ransomware or extortion demands. The survey — conducted by Rubrik Zero Labs across over 1,600 security leaders — highlights that almost all victims paid extortion demands, reflecting both the high frequency of ransomware targeting Australian entities and the pressure organisations face when critical systems or data are held at risk. Attackers are not just encrypting systems anymore; data theft and public-leak threats have become equally central to extortion playbooks. For executive leaders, this reinforces the urgency of strengthening ransomware prevention and response postures — from robust offline backups and incident tabletop exercises to negotiated approaches with insurers and law enforcement — and elevating ransomware readiness to a boardroom and risk-management priority.

Services Australia may get powers to rein in data breach exposure

Services Australia may gain stronger powers to compel rapid disclosure when third parties suffer breaches involving government identifiers like Medicare and Centrelink numbers. iTnews says this is driven by rising notifiable breaches linked to criminal activity, including scams where people are tricked into surrendering myGov credentials. A key gap is that Services Australia reportedly can't currently force timely information-sharing from breached partners, even when exposed identifiers increase identity-fraud risk. The federal auditor has recommended reforms, with the OAIC and Attorney-General's Department broadly supportive, signalling tighter reporting expectations and greater scrutiny of supply-chain breaches that can impact citizens at scale.

World

Hackers breach internal servers of tech provider for Britain's health service

DXS International, a UK tech supplier whose software is widely used across the NHS, disclosed a cyber incident affecting its internal systems. While there's no confirmed impact to NHS operations in early reporting, the case highlights how third parties can become gateways into larger ecosystems or expose sensitive service workflows. For executives, the key risks are service disruption if the vendor's delivery capability is degraded, and potential exposure of data or credentials that could be leveraged against customers. Recommended actions include treating critical vendors as part of the extended enterprise: enforce timely incident-notification obligations, verify strong segregation between vendor and customer environments, and retain the ability to quickly restrict or disable integrations if a supplier is compromised. It also reinforces the value of maintaining a clear critical-supplier register and regularly exercising supplier-incident response via tabletop scenarios.

India records 265 million cyber attacks in 2025: Report

A comprehensive threat report from Seqrite Labs revealed that India faced over 265 million cyber-attacks in 2025, indicating a surge in malicious digital actions across sectors. The study covered a range of attack types from malware campaigns to brute force and exploitation of vulnerabilities affecting enterprises, critical digital services and government networks. In response to this elevated threat environment, Seqrite introduced new enterprise cybersecurity services focused on ransomware recovery and digital risk protection, reflecting a strategic shift toward resilience and rapid recovery. This report underscores the volume and velocity of cyber threats in one of the world's fastest-digitising economies and highlights the need for robust incident detection, automated defense, and cross-sector coordination to strengthen national cyber posture.

Interpol-led cybercrime crackdown results in 574 arrests in 19 African nations, decrypts six ransomware variants — Operation Sentinel disrupts rings that caused $21 million in losses, recovers $3 million

INTERPOL's "Operation Sentinel" disrupted cybercrime across 19 African countries, resulting in 574 arrests linked to BEC, digital extortion and ransomware. Authorities dismantled over 6,000 malicious links, decrypted six ransomware variants, and recovered about USD 3 million. The operation also uncovered major cases including a blocked USD 7.9 million BEC attempt against a Senegalese petroleum firm and a Ghana ransomware incident involving 100TB of data, highlighting the impact of coordinated cross-border enforcement on cybercrime networks.

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.

18/12/2025 – Active exploitation of vulnerabilities in multiple Fortinet products

Our Views:

Incident Response Preparedness Is Now a Baseline Expectation

Last month's bulletin highlighted a clear shift in New Zealand's operating environment. With the release of updated Government guidance on the Minimum Cyber Security Standards, the message was unambiguous: security maturity is no longer optional, and reactive incident response is no longer acceptable.

These standards are positioned as a baseline. They assume that organisations can detect malicious activity, understand what is at risk, and coordinate an effective response across technology teams and the wider business. Where that capability does not exist, organisations are exposed not only to cyber risk, but to regulatory, reputational, and governance consequences.

"Minimum" does not mean easy. It means expected. If you cannot quickly identify abnormal behaviour, retain and access the right evidence, or make timely decisions during an incident, you are already behind the curve.

The context has changed again, and scrutiny is rising

During the Christmas holidays, the Government commissioned a review into the Manage My Health cyber security breach. The review is examining the causes of the incident, the adequacy of security controls, and the effectiveness of the response, with the explicit aim of preventing similar events in the future.

This is an important signal. Cyber incidents are no longer viewed purely through a technical lens. They are treated as whole-of-organisation events, with scrutiny extending into governance, preparedness, decision-making, and accountability.

Recent high-profile breaches reinforce the same lesson. Once an incident becomes public, attention quickly shifts from what happened to how it was handled. **In that environment, a breach is judged not just by its occurrence, but by the speed, clarity, and confidence of the organisation's response.**

In this environment, preparedness is no longer an IT responsibility alone. It is a leadership obligation.

Preparedness is not documentation. It is a capability.

Many organisations still equate incident response readiness with having a document on the intranet. In practice, preparedness is demonstrated through behaviour under pressure.

Prepared organisations can:

- recognise an incident quickly, even when signals are ambiguous,
- prioritise the right systems and data based on business impact,
- make confident decisions with incomplete information,
- coordinate technical, legal, communications, and executive actions, and
- show evidence, after the fact, that response actions were reasonable, timely, and proportionate.

Unprepared organisations struggle with authority, lose time debating next steps, and default to improvisation. That gap is increasingly visible to regulators, customers, and Boards.

Four steps organisations should action now

1. Incident Response Planning: publish and maintain a fit for purpose plan

A cyber incident response plan is the organisation's pre-agreed operating model for crisis conditions. It defines how decisions are made, who leads, how escalation occurs, and how response activities are coordinated.

Without a current and practical plan, response efforts quickly fragment. Authority becomes unclear, critical evidence is mishandled, and valuable time is lost during the most sensitive phase of an incident. A fit for purpose plan should be:

- aligned to your actual business risks and critical services,
- understood at both operational and executive levels,
- supported by scenario-based playbooks for realistic threats, and
- reviewed regularly, not just after a breach.

Plans should evolve as systems change, threats shift, and lessons are learned from exercises and real incidents.

Reference: https://incidentresponse.co.nz/incident-response-plan/

2. Tabletop Simulations: test decision-making, not documentation

A plan that has never been exercised remains theoretical.

Tabletop simulations are where preparedness is validated. They test how people actually behave when timelines compress, information is incomplete, and trade-offs must be made between containment, recovery, legal exposure, and public communication.

Effective simulations:

- involve executives, legal, communications, and system owners, not just IT,
- focus on decisions and consequences rather than technical walkthroughs,
- surface hidden dependencies and assumptions, and
- build shared understanding of roles under pressure.

For many leadership teams, a well-run simulation is the first time they experience the organisational and decision-making strain of a serious cyber incident. That experience is difficult to replicate any other way, and invaluable when a real incident occurs.

Reference: https://incidentresponse.co.nz/cyber-incident-simulations/

3. Post Incident Review: lock in the learnings, or repeat the incident

Too many organisations treat incident closure as the end of the process. In reality, it is the most important transition point.

A post-incident review ensures that effort spent responding results in improved resilience. Without it, the same weaknesses tend to reappear, often in the next incident.

A strong post-incident review should:

- clearly reconstruct the timeline, including detection, escalation, and decision points,
- identify root causes rather than symptoms,
- assess what worked and what failed across technical and business response,
- present findings in a format executives and Boards can act on and translate recommendations into tracked remediation actions.

Post-incident reviews should occur after material incidents and major exercises, and they should directly inform updates to plans, playbooks, and training.

Reference: https://incidentresponse.co.nz/post-incident-review/

4. Incident Response Retainer: secure year-round capability before you need it

One of the most common failure points in cyber incidents is attempting to secure specialist support during the crisis itself. At that point, organisations are under intense time pressure, internal stress is high, and external scrutiny may already be building. Delays while availability, scope, or contracts are negotiated can materially worsen outcomes.

An incident response retainer removes that risk by establishing access to expertise and essential services in advance. This typically includes readiness support, access to experienced responders, operational coordination tools, and defined engagement pathways that can be activated immediately when needed. From an executive perspective, a retainer is less about cost efficiency and more about certainty of response.

Reference: https://incidentresponse.co.nz/incident-response-retainer/

Executive Expectations and Call to Action

At an executive level, strong incident response preparedness is demonstrated when roles and decision authority are clear, leaders have practised responding under pressure, response capability is proven rather than assumed, and lessons from incidents are converted into measurable improvement. This is now the standard stakeholders expect.

Against the backdrop of clearer Government baselines, ongoing high-impact breaches, and an active Government-commissioned review into cyber preparedness, organisations should act now, not after the next incident. Preparedness must be treated as an ongoing leadership discipline, supported by a current incident response plan and risk-aligned playbooks, regular tabletop simulations, disciplined post-incident reviews, and assured access to specialist response capability.

In today's environment, the question is not whether an incident will occur, but whether your organisation will be ready to respond when it does.

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: