NZ Incident Response Bulletin

Standard Edition – November 2025 – Issue #82

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

Windows 10 support ends: '30% of NZ computers at risk'

As of 14 October 2025, Microsoft has officially ended free support and security updates for Windows 10, leaving an estimated 30% of New Zealand computers exposed to increased cybersecurity risks. This move affects millions of users whose devices may no longer receive critical patches, making them more vulnerable to malware, ransomware, and other cyber threats. For those whose hardware doesn't support Windows 11, options are limited: they must either invest in new computers, switch to a different operating system, or enrol in Microsoft's Extended Security Updates programme. While some users may access the extended support for free, it requires manual enrolment and does not offer the same level of protection as a fully supported operating system.

Cyber security agency's new website reveals how many times NZ logons have been leaked - and where

The National Cyber Security Centre (NCSC) has launched "How Exposed Am I?", a public tool that allows New Zealanders to check how many times their login details have appeared in known data breaches. The service uses data from Have I Been Pwned and provides tailored NCSC guidance to help users understand risks and improve their security. The launch comes amid rising cyber losses, with more than 830,000 New Zealanders reporting financial harm from cyber incidents and an average loss of around NZ$1,260 per event. The initiative aims to challenge public complacency by showing that even old breaches remain dangerous, as leaked credentials often circulate for years on the dark web. The campaign aligns with Cyber Smart Week and reinforces best-practice behaviours, including using strong and unique passwords, enabling multi-factor authentication, employing password managers, and avoiding sensitive activity on public Wi-Fi.

Australia

Qantas hack: Data from 5.7 million customers posted online after cyber attack

Qantas Airways confirmed that data from approximately 5.7 million customers was stolen in a cyberattack that targeted a third-party customer service platform. The exposed information included names, email addresses, frequent flyer numbers, and in some cases, phone numbers, dates of birth, and physical addresses. Qantas stated that no credit card details, passport numbers, or login credentials were compromised. The hacker group responsible, identified as Scattered Lapsus$ Hunters, published over 150 GB of the stolen data on the dark web after a ransom deadline passed. The breach has raised serious concerns about data security and highlighted the vulnerabilities associated with outsourcing customer service functions, particularly the risk of social engineering and inadequate protections in third-party environments.

Tax file numbers and health information: Western Sydney University suffers major cyber breach

Western Sydney University (WSU) suffered a serious cyber breach between June 19 and September 3, 2025, during which hackers exploited a cloud-based student management system hosted by a third-party and linked external providers. The attackers accessed a wide array of sensitive personal data including tax file numbers, bank and payroll details, driver's licence and passport information, visa status, health and disability records, legal case information, and more. WSU is working with the NSW Police Force Cybercrime Squad's Strike Force Docker, has notified affected individuals, and has committed to enhancing its cybersecurity posture and support services for its community.

World

Capita fined £14m for data breach affecting over 6m people

Capita has been fined £1.4 million by the UK's Information Commissioner's Office (ICO) for failing to adequately protect personal data in a breach that affected more than six million people. The breach occurred when Capita left a cloud-based storage system unprotected online for over three years, exposing sensitive personal information linked to around 90 organisations, including local councils and pension funds. The ICO described Capita's security controls as "inadequate," especially given the volume and sensitivity of the data involved, which included names, addresses, and in some cases, financial and benefits information.

The exposed data was accessible online without any authentication, a basic lapse in security practice that the ICO found unjustifiable. While the breach was not caused by a cyberattack, the regulator noted that Capita's poor handling of the storage configuration created unnecessary risk. The incident has drawn sharp criticism and serves as a warning to other organisations that handle large volumes of personal information, particularly public sector contractors. It also highlights the ICO's increasing readiness to issue significant penalties where poor data governance exposes individuals to harm.

'I lost 25 pounds in 20 days': what it's like to be on the frontline of a global cyber-attack

In December 2020, SolarWinds was at the center of a major cyberattack when hackers linked to Russian intelligence infiltrated its Orion network-monitoring software. This software was widely used by over 300,000 organizations globally, including key U.S. government agencies. The company's Chief Information Security Officer, Tim Brown, described the early days of the incident as a crisis—staff had to disable internal systems, move to secure communication tools, and operate under immense pressure with global attention focused on their every move. The article also details the severe personal toll the breach took on Brown, who lost significant weight, struggled with sleep, and eventually suffered a heart attack from the prolonged stress. It highlights how cyberattacks don't just challenge technical systems—they test the resilience, leadership, and health of the people managing the response. The story is a sobering reminder of the human cost behind high-profile breaches and the need for crisis readiness that accounts for both technology and well-being.

Noosa mayor says fraudsters used AI imitation in $2.3m council scam

Noosa Council in Queensland disclosed that it was defrauded of approximately A$2.3 million in December 2024 through a sophisticated international scam. While about A$400,000 was later recovered, the net financial loss remains close to A$1.9 million. Importantly, there was no breach of the council's internal IT systems and no personal data was compromised. The stolen funds were transferred offshore very quickly, consistent with tactics used by organised cybercriminals in business email compromise and social engineering schemes.

Mayor Frank Wilkie said the scammers likely used AI tools to convincingly imitate people within the organisation, manipulating staff into authorising the fraudulent payments. This reflects a growing trend of cyber threats that rely more on human deception than technical system exploitation. The council confirmed that no employees were held responsible and normal services were not impacted. The incident has drawn attention to the risks of AI-enabled fraud, particularly in public sector operations where trust and communication protocols can be exploited.

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.

28/10/2025 – Critical vulnerability in Microsoft Windows Server Update Service (WSUS)

Our Views:

NZ Government's Cyber Rules Are Clear – Is Your Incident Response Ready?

The New Zealand Government has stepped up its expectations. With the release of new cyber guidance on Minimum Cyber Security Standards, Risk Management, and the INFOSEC Policy from the Protective Security Requirements (PSR), the message is clear: security maturity is no longer optional, and reactive incident response won't cut it.

This isn't just advisory material to file away; it's a clear signal of the baseline organisations are now expected to meet. Agencies, Crown entities, and businesses working with or alongside government need to sit up. The days of 'we'll deal with it when it happens' are over.

Minimum Standards Mean Just That – Minimum

The new baseline requires enforceable configurations, hardened perimeter controls, and system-level visibility. If your Security Operations Centre (SOC) can't detect unusual behaviour fast, or worse, if logs aren't even retained, you're already out of compliance. These aren't aspirational goals; they're mandatory expectations. Incident response must plug directly into these controls, or else it will fail when it matters most.

Risk Isn't a Buzzword – It's the Operating Model

The updated risk management guidance pushes organisations to prioritise based on actual threat exposure and business impact. Incident response needs to reflect that. No more cookie-cutter playbooks. If your crown jewel systems or citizen data repositories aren't mapped and prioritised in your response strategy, you're flying blind.

The INFOSEC Policy Lays Down the Governance Line

This is where accountability becomes critical. If information isn't appropriately classified and protected, or if business owners are not clearly engaged in the response process, the organisation may fall short of the expectations outlined in the Protective Security Requirements. In the event of a cyber incident, any gaps in preparation or unclear roles can quickly escalate into a governance issue—placing significant pressure on senior leadership to explain why response capabilities didn't meet the required standard.

What Should Organisations Actually Be Doing?

- Get Honest About Detection Gaps: Stop assuming your monitoring works and test it. Validate alerting, response times, and access visibility across your most critical systems.
- Rewrite Your Playbooks Around Risk: Generic plans won't help when you're dealing with real-world ransomware or insider threats. Build scenarios based on your threat model, not someone else's.
- Stress Test with the Right People in the Room: Your response plan is only as strong as the people executing it. Include execs, legal, comms, and system owners in exercises. If they can't make the right calls under pressure, fix it.
- Enforce Role Clarity Across the Business: If nobody knows who leads during an incident, or what data is most important, response time doubles and consequences multiply.
- Treat Compliance as Evidence, not a Paper Exercise: Be ready to demonstrate how your plans, capabilities, and governance align with government expectations. This is now part of the trust equation, especially in public sector and regulated environments.

The Bottom Line

The NZ Government has drawn a line. These updated standards and policies are the floor not the ceiling. If your incident response capability can't confidently detect, prioritise, and coordinate a whole-of-business response to cyber threats, you're behind. And in today's threat landscape, behind quickly becomes breached.

Contact us if you need to discuss how to make the necessary improvements to your incident response processes.

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

This Bulletin is prepared for general guidance and does not constitute formal advice. This information should not be relied on without obtaining specific formal advice. We do not make any representation as to the accuracy or completeness of the information contained within this Bulletin. Incident Response Solutions Limited does not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, when relying on the information contained in this Bulletin or for any decision based on it.

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: