



NZ Incident Response Bulletin

Standard Edition - October 2026 - Issue #93

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 will 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 are not caught by surprise and you know about risks and changes before they become problems. For readers wishing to receive additional Forensic and Cyber Security information, our Premium Edition is available to clients subscribed to our Incident Response Retainer.

News:

A high-level executive summary containing some of the most important news articles published on Forensic and Cyber Security matters during September 2026.

New Zealand

[New Zealand identifies China as its most persistent state-backed cyber threat](#)

The New Zealand's National Cyber Security Centre identified China as the most persistent and capable state-backed cyber threat operating against the country. The NCSC's Cyber Threat Report linked suspected activity to actors from China, Russia, Iran and North Korea, and said 86 of 369 incidents of potential national significance in the year to June 2026 had suspected state-sponsored links. Targets included government, health, education and information-technology organisations. China rejected the assessment. The NCSC warned that espionage activity may remain hidden for months or years while an actor conducts reconnaissance and positions access. Organisations should treat unusual identity, supplier and remote-access activity as possible evidence of a longer campaign, preserve logs for meaningful periods and use threat-informed investigation rather than waiting for disruption or data publication.

[NZ cyber threat report warns of rising risk from AI turbo-charging crime](#)

New Zealand's National Cyber Security Centre is warning that artificial intelligence is making cybercrime faster, more scalable and more convincing. Attackers are increasingly using AI to support phishing, reconnaissance, deepfakes and vulnerability exploitation. The NCSC says organisations should continue focusing on strong cyber security fundamentals, including multi-factor authentication, timely patching, secure access controls and tested incident response plans. As AI accelerates the speed of attacks, businesses will need to detect, respond to and recover from cyber incidents more quickly.

[Privacy Commissioner orders remediation after Manage My Health breach](#)

The Privacy Commissioner issued compliance notices to Manage My Health and Health New Zealand on 23 September over security failures associated with the December 2025 patient-portal breach. The Commissioner identified seven areas where protections had been ineffective. Manage My Health had already improved multifactor authentication, restricted user access and controls over unauthorised external access, but further work remained. Health NZ must complete its required changes by 29 January 2027, while Manage My Health has until 31 August 2027 to complete all requirements. The notices apply both to the service provider and to the organisation that supplied health information to it. The governance lesson is direct: an organisation cannot rely on limited technical visibility as a reason for weak oversight. Due diligence, contractual safeguards, risk ownership and continuing assurance must be strong enough for the sensitivity of the information entrusted to a provider.

Australia

[Mathspace breach affects more than one million users across Australia and New Zealand](#)

Education provider Mathspace said unauthorised parties accessed an internal reporting system between 10 and 27 August while a security patch had not been installed. ABC News reported on 7 September that 1,079,819 students, parents, teachers and staff in Australia and New Zealand were affected. Exported fields included names, email addresses, user types, countries, time zones and account activity dates. Mathspace said academic records, assessment results, passwords, authentication tokens, single-sign-on credentials and API credentials were not exposed. The compromised system was taken offline and affected people were being contacted. The event illustrates how a secondary reporting database can create a large affected population even when core learning records remain separate. Schools and technology providers should confirm ownership of patching, minimise reporting-system retention and be ready to explain clearly which fields and credentials were not involved.

[OpenAI apologises after experimental agent accesses Australian government portal](#)

OpenAI said an experimental AI model obtained unauthorised non-public access to the Services Australia Medicare Statistics Reporting Service during an internal training activity in June. The agent ran commands, retrieved internal files, credentials and aggregate statistics, and wrote files. OpenAI said its review had found no evidence that medical records were accessed, and activity affecting three other Australian government websites did not expose sensitive records. The incident became public in September after criticism of the notification delay and route. OpenAI apologised, promised support for affected agencies and an Australian taskforce, while the government began a rapid review of legal and reporting obligations. This is a material new development from the agent incidents reported in the previous Bulletin. Organisations testing autonomous systems should use isolated environments, explicit target restrictions, independent monitoring and immediate human escalation when an agent crosses an authorisation boundary.

World

[ShinyHunters renews mass exploitation of Oracle PeopleSoft](#)

Google's Mandiant unit reported on 25 September that ShinyHunters had renewed mass exploitation of a vulnerability in Oracle PeopleSoft. The group had previously exploited the flaw between 27 May and 9 June, mainly against universities, then adapted after defenders deployed web-application firewall rules without installing Oracle's update. Mandiant said the latest activity affected dozens of systems across education, technology, healthcare, agriculture, transport and government. The FBI was investigating a claim that its personnel data had been accessed through PeopleSoft, although Reuters could not verify that claim. The operational lesson is that a compensating control is not a permanent substitute for remediation. Organisations using PeopleSoft should confirm the actual patch level, review internet exposure and historical logs, and investigate for compromise rather than treating a firewall rule as proof that the vulnerability was neutralised.

[Bitget suspends withdrawals after US\\$351.6 million cryptocurrency theft](#)

Cryptocurrency exchange Bitget suspended customer withdrawals after detecting unauthorised transfers worth approximately US\$351.6 million from some of its wallets. The company said on 25 September that all customer funds were safe, the loss would be covered from its own resources and the withdrawal pause was a security precaution rather than a liquidity issue. Bitget says it serves more than 120 million users. At the time of reporting, the public information did not establish the access route or responsible actor. The incident demonstrates the speed at which digital assets can move across borders and the importance of separating containment from solvency messaging. Exchanges and other organisations controlling transferable digital value should use independent approval for high-risk transfers, pre-authorised wallet isolation procedures, real-time monitoring and communications that distinguish confirmed customer impact from the organisation's ability to absorb a loss.

Summary of September's Cyber Alerts and News Clips

Incident Response Solutions posts selected alerts and tips that we consider to be in the public interest. We publish these alerts and tips on this webpage.

- [28/09/2026 - Actively exploited vulnerabilities affecting Citrix NetScaler products](#)



NZ Incident Response Bulletin

Standard Edition - October 2026 - Issue #93

Our Views:

Incident Arena: Adding a New Dimension to the Tabletop Exercise

Key Takeaway: Incident Arena is our new crisis simulation solution for executive and leadership teams. It keeps everything that makes a facilitated tabletop valuable, the discussion, the debate and the debrief, and adds what paper can't: a clock that keeps running, consequences the room can see, a budget that won't stretch to everything, and a record of every decision. We look forward to bringing it to our clients.

In our May bulletin we wrote about cyber simulations and tabletop exercises, and about the growing demand from experienced clients for exercises that feel closer to a real incident: more pressure, less certainty and more at stake in each decision. Incident Arena is our answer to that demand. It does not replace the facilitated tabletop. It gives it a new dimension.

One shared screen, one collective decision

Incident Arena is run by an Incident Response Solutions facilitator, in the room, on one shared screen. The team works through a realistic cyber incident as it unfolds. At each inject, a new development in the incident, the team reads the situation, discusses its options and agrees one answer from four plausible choices before the timer runs out. Each inject shows which role leads the discussion, so the right voices are heard at the right time. The facilitator can pause the clock at any point to draw out a conversation, and the team can record the reasoning behind each decision.

If the clock runs out, that has consequences too. As in a real incident, not deciding is itself a decision.

Consequences you can see

The defining feature of Incident Arena is five live health dials: operational resilience, data protection, financial health, reputation and regulatory compliance. After every decision the dials move, with the reason for each change. A well-judged containment decision may protect operations but cost money; a delayed notification may save time today and damage regulatory standing tomorrow. If a dial reaches zero, play can stop, just as a real crisis can overwhelm an organisation. In a traditional tabletop, the impact of a decision lives in the discussion and in the facilitator's notes. In Incident Arena the whole room sees it the moment it happens. That changes the conversation. Trade-offs become concrete, quieter participants have something specific to respond to, and the link between a decision and its organisational impact becomes hard to ignore.

Real trade-offs, real constraints

Between injects the team can spend a limited response budget on specialist support such as digital forensics, legal and privacy advice, crisis communications or an incident response surge team. Some support takes time to arrive, so timing matters as much as choice. A cyber insurance policy can pay back part of what it covers, as it would in practice. The budget never stretches to everything, which forces exactly the conversations organisations need to have before an incident, not during one: what do we need first, who authorises the spend, and what are we prepared to go without?

Scenarios that fit the room

The first edition of Incident Arena includes ten scenarios reflecting the attacks New Zealand organisations face, including ransomware, business email compromise, cloud account takeover, data theft and extortion, supplier compromise, a malicious insider, an attack on operational technology, and AI impersonation and social engineering. Each can be played by a full incident response team or focused for a technology and cyber team, a communications team or the board, and some have versions tailored to particular industries. We set the severity, the starting health of the organisation, the time allowed for each decision and the roles in the room, so the exercise matches the maturity and make-up of the team.

Built for the debrief, and for doing it again

At the end, the results show where each dial started and finished, every decision and its impact, and what was bought. Your facilitator leads the debrief and exports a report covering the decisions, their impact, the budget and insurance, and recommended next steps, and each team receives a certificate of completion. Because every session is recorded in the same way, Incident Arena is well suited to the repeat programmes we advocated in May. Run the same scenario a year later and compare. Is the team deciding faster? Are the dials ending higher? Are the same gaps appearing? That gives boards and executives a tangible view of how their crisis decision-making is maturing over time.

Private by design

Incident Arena runs entirely offline on our own device, with no need for an internet connection, cloud services or accounts, and session records stay with us. The health dials are an exercise device to drive discussion, not predictions of loss or findings of legal compliance.

Tabletop exercises remain one of the most effective ways to build cyber resilience, and the facilitated discussion will always be at their heart. Incident Arena adds time pressure, visible consequences and genuine trade-offs to that discussion, and leaves a record the organisation can build on. We are excited to begin delivering Incident Arena to our clients and look forward to running it with your team. To find out more, or to discuss how Incident Arena could fit your next simulation exercise, contact us at support@incidentresponse.co.nz. You can also watch our [launch video here](#).



NZ Incident Response Bulletin

Standard Edition - October 2026 - Issue #93

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:

