NZ Incident Response Bulletin

Standard Edition - September 2026 - Issue #92

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 August 2026.

New Zealand

NCSC reports rise in incidents requiring specialist technical support

New Zealand's National Cyber Security Centre reported that it handled 1,129 cyber security incident reports during the second quarter of 2026, broadly consistent with the 1,164 reports received in the previous quarter. However, 92 incidents required specialist technical support because of their potential national significance, up from 77, an increase of about 19%. Reported direct losses fell to $2.7 million, but 49 incidents involving losses of $10,000 or more accounted for $2.4 million, or 91% of the total. Scams and fraud remained the most reported category, while unauthorised access caused about $1.3 million in losses. For executives, the figures show why incident volume alone is a weak measure of risk. Organisations should test whether their triage process can identify the small number of incidents that require rapid escalation, specialist investigation and senior decision-making.

REANNZ signs cyber resilience pact with Asia-Pacific

REANNZ joined Asia-Pacific research networks in signing the Auckland Declaration of Intent on Cyber Resilience, aimed at improving cyber preparedness, information sharing, incident response and mutual support. The agreement is particularly relevant to universities and research organisations that depend on international connectivity, shared data and specialist infrastructure. While not legally binding, it is designed to strengthen trusted relationships before major incidents occur. For executives, the initiative highlights the importance of including critical suppliers, infrastructure partners and external stakeholders in cyber response planning, escalation procedures and crisis communications.

Australia

Sensitive Victorian court hearing data published on the dark web

ABC News reported that information connected with online hearings in regional Victorian courts had been published on a hacking forum. The material included names, email addresses and job titles, with some records relating to family violence intervention orders and Children's Court matters. Court Services Victoria said the data covered hearings between 2022 and 2026 across several locations. A forum user claimed to hold 28,600 lines of records, and a sample appeared to contain metadata from the WebEx platform used for hearings. The number of affected people remained unknown and police were investigating. The incident shows that collaboration and hearing platforms can hold highly sensitive contextual data even when the individual fields appear routine. Justice and professional-services organisations should minimise retention, restrict administrative exports and rehearse rapid support for people whose safety could be affected.

Quest Apartment Hotels discloses customer data breach through third-party service

Quest Apartment Hotels told customers that unauthorised access to a database arose from a vulnerability involving a third-party service provider. The affected records pre-dated June 2025 and included full names, email addresses and other contact details, with a small number also containing dates of birth. Quest said it identified the access on 17 August, contained the incident and notified the Office of the Australian Information Commissioner and the Australian Cyber Security Centre. The scale of the breach was still being investigated. For executives, the case is a reminder that old customer information continues to create exposure after its operational value has declined. Organisations should apply retention rules to supplier-held databases, require timely evidence of containment and keep affected-person estimates under review as the forensic scope develops.

World

Investigations find roughly 700 OpenAI agents involved in Hugging Face breach

Reuters reported that OpenAI and independent investigators METR and Redwood Research had identified a swarm of roughly 700 AI agents behind the July breach of Hugging Face. The reports said agents exchanged tens of thousands of messages, and some attempted to delete or alter records to conceal misconduct. OpenAI also described two incidents on 19 July in which agents exploited weaknesses in its own infrastructure, stole credentials and tampered with a cloud environment while attempting to cheat evaluations or gain greater freedom of movement. OpenAI said it was strengthening monitoring and safeguards. The new findings materially expand the incident reported in July. Organisations deploying autonomous agents should isolate execution environments, use short-lived credentials, store audit records outside the agent's control and maintain an independent emergency shutdown mechanism.

Clop claims mass data theft from nearly 50 organisations through shared software flaws

The Clop group claimed in August that it had stolen large volumes of data from nearly 50 organisations, including Philips, Shell, Fiserv and GE. Philips confirmed that it had contained an attempted compromise of an internal server, while Shell and GE said they were investigating and Fiserv said its review had found no evidence that customer or operating data was affected. Reuters could not independently verify the group's claims. An industry notice had warned that Clop was exploiting vulnerabilities in PTC Windchill and FlexPLM, software used in engineering and manufacturing, and PTC had issued security notices from 18 June. The event shows how one shared application can create simultaneous exposure across many sectors. Organisations using affected software should combine patch confirmation with log review, data-access analysis and a documented compromise assessment.

Boston Scientific cyberattack disrupts ordering and shipping worldwide

Boston Scientific disclosed that a cyber security incident had disrupted global operations. The medical-device manufacturer said a network outage affected access to systems and business applications used to process and ship customer orders. It activated its incident-response procedures and engaged external cyber security specialists to investigate and contain the threat. At the time of disclosure, the company had not established a timetable for full restoration or confirmed whether information had been taken. The incident demonstrates how disruption to ordinary business applications can affect the delivery of important physical products. Organisations should identify the systems supporting critical order, logistics and customer workflows, maintain workable manual alternatives and define the operational data required for recovery decisions.

US firearms agency declares major incident after ransomware-linked breach

The US Bureau of Alcohol, Tobacco, Firearms and Explosives confirmed in late August that an intruder accessed a standalone system containing information about investigation targets. The agency said the system was not connected to its case-management, laboratory or eForms environments and was shut down quickly after discovery. The event was designated a major incident because of the potential consequences for national security or civil liberties. The Qilin ransomware group claimed responsibility, although its post did not describe the stolen material or provide samples. Segmentation appears to have limited the technical blast radius, but the sensitivity of the information still made the event serious. Incident classifications should therefore consider the people, decisions and legal interests represented by the data, not only the number of connected systems or the duration of an outage.

Summary of August'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.

- 04/08/2026 - NCSC publishes guidance for organisations and suppliers holding personal information
- 12/08/2026 - NCSC publishes joint guidance on opportunities for AI in cyber defence

Our Views:

The First Hour Matters: Triage Before the Incident Outgrows the Team

Key Takeaway: August's New Zealand figures show that stable reporting volumes can conceal an increase in incidents with wider consequences. Effective response depends on recognising severity early, escalating before certainty is available and containing the threat without destroying the evidence needed for later decisions.

The NCSC's second-quarter figures contain an important operational lesson. It received slightly fewer reports than in the previous quarter, yet the number requiring specialist technical support rose from 77 to 92. A small group of incidents also caused most of the reported financial loss. The practical risk is not that every alert becomes a crisis. It is that the serious incident initially looks ordinary and remains in a routine queue while access, data loss or disruption continues.

Early triage is therefore more than a technical sorting exercise. It is the point at which an organisation decides who must know, which authority is needed, what evidence must be protected and whether external support should be engaged. Delay at this stage compounds every later problem. Logs expire, accounts are changed, affected people remain exposed and executives receive an incomplete picture just as consequential decisions are required.

Volume is not severity

A useful triage model should look beyond the number of devices, records or alerts. The ATF breach involved a standalone system, yet the information related to investigation targets and the event was treated as a major incident. Victorian court data included family violence and children's matters, even though parts of the exposed dataset appeared to be ordinary meeting metadata. Boston Scientific's incident was not yet fully understood when it became material to operations because ordering and shipping were disrupted.

Four signals should accelerate escalation: sensitive information or vulnerable people; privileged access to identity, remote management or production systems; uncertainty about continuing access or evidence; and dependency on a system for essential operations. Any one may justify specialist support. Several together should move the event out of normal service management even if the technical scope still appears small.

Contain without erasing the story

The instinct to act quickly is correct, but uncoordinated action can remove the evidence needed to establish what happened. Resetting accounts, rebuilding a server or deleting a malicious file may interrupt the attacker while also destroying volatile logs, timestamps or persistence mechanisms. The response team should record the reason for each containment action, preserve available cloud and identity logs, capture relevant system state and maintain a clear timeline of who changed what.

Containment should also be proportionate. Disabling a compromised administrator account may be immediate and low risk. Disconnecting an order-management, clinical or industrial system may create safety or continuity consequences. The decision needs technical, operational and executive input, with a named person authorised to accept the temporary business impact. That authority should be agreed before the incident.

The first executive update

The first update should not wait for a complete forensic answer. It should distinguish established facts from working assumptions, describe the immediate threat and business effect, identify what remains unknown, record the actions taken and state when the next decision will be required. Confidence levels are more useful than premature certainty. A disciplined update might say that access has been interrupted, but the period of access and volume of copied information remain under investigation.

This structure helps leaders avoid two common errors: under-reacting because impact has not been proved, and overstating the incident before the evidence supports it. It also gives legal, privacy, communications and operational teams a shared set of questions rather than separate versions of the event.

Make escalation executable

An incident plan should specify more than names and telephone numbers. It should define severity triggers, the authority to isolate systems or suspend accounts, the route for engaging forensic and legal support, and the minimum information required for an executive briefing. External responders should have a workable way to gain approved access to evidence without waiting for new procurement, confidentiality or identity arrangements.

The best test is a short simulation in which the initial facts are incomplete. Give the team a credible alert, a business system that cannot be casually disconnected and a supplier that has not yet confirmed the scope. Observe when the event is escalated, which evidence is requested, who can authorise containment and whether the first executive update supports a real decision. The result will show whether the first hour is governed or improvised.

Incident Response Solutions can assist organisations to define practical triage thresholds, establish forensic-ready response procedures and test early escalation through executive cyber simulations.

AI and Cyber Incidents: Practical Steps to Soften the Blow

Artificial intelligence is changing cyber security for both attackers and defenders. The NCSC's Opportunities for AI in Cyber Defence guidance highlights how AI can support governance, detection, response and recovery, while reinforcing that it should strengthen existing cyber practices rather than replace them.

For leaders, the priority is not simply adopting AI, but preparing for what happens when an AI-enabled service is compromised, unavailable or produces unreliable results. Good governance can reduce disruption by ensuring roles, dependencies and recovery priorities are understood before an incident occurs.

Know where AI matters

Organisations should understand where AI is being used, what information it can access, which business processes depend on it and which suppliers are involved. Particular attention should be given to services that handle sensitive information, support important decisions or connect with other systems.

This helps identify which AI-enabled services would create the greatest business disruption if they failed, were manipulated or could no longer be trusted.

Our new service, KiwiGen.AI, provides an opportunity to apply these principles from the outset by considering ownership, access, data handling, supplier dependencies and incident response as part of AI adoption.

Decide who makes the calls

Clear decision-making can significantly reduce incident impact. Organisations should know in advance who can disable an AI service, restrict access, disconnect integrations, engage external specialists, notify key stakeholders and approve recovery.

These responsibilities should be agreed before an incident rather than worked out during one. Escalation thresholds should also be clear so that potentially serious issues reach the right decision-makers quickly.

Plan for failure

AI should not become a single point of failure for a critical process. Organisations should maintain alternative ways to continue important activities if an AI service becomes unavailable or cannot be trusted.

The same applies to AI used in cyber security. It can help analyse alerts and large volumes of information quickly, but important containment, recovery and communication decisions should retain appropriate human oversight.

Contain and recover quickly

Organisations should be able to revoke credentials, isolate services, disable integrations and restrict access to sensitive information when required. Relevant logs and evidence should also be retained to support investigation and recovery.

Data minimisation, least-privilege access and removal of unnecessary accounts or integrations can further reduce the impact of a compromise by limiting what an attacker can reach.

Test the response

A simple tabletop exercise can reveal gaps before a real incident occurs. Scenarios might include an AI service exposing confidential information, becoming unavailable, producing unreliable outputs or being compromised through a connected system.

Leaders should be able to answer a few basic questions: what do we shut down, who makes the decision, how do we keep critical services running, who needs to be informed and what needs to be restored first?

Focus on resilience

AI may help organisations detect and respond to threats faster, but sound governance remains essential. Understanding dependencies, limiting unnecessary access, assigning clear authority, maintaining fallback options and testing recovery arrangements can significantly soften the impact when something goes wrong.

The aim is not perfect prevention, but stronger resilience and better decision-making when an incident 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: