NZ Incident Response Bulletin

Standard Edition - November 2026 - Issue #94

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 that have been published on Forensic and Cyber Security matters during the last month.

New Zealand

'Serious misconduct': Officer's repeated online searches for influencers

A senior New Zealand Police officer was found to have committed serious misconduct after repeatedly using a work device to search for a small group of female social media influencers. The Independent Police Conduct Authority said the searches were conducted both on and off duty and were notable for their volume and repeated focus on particular accounts. Cybersecurity investigators were brought in to collect digital evidence of the searches and material viewed. The case emerged from a wider review of Police-issued devices and information security controls, launched after concerns about inappropriate material being accessed on work equipment. Police determined the officer's behaviour breached policy and the code of conduct, while a broader technology review identified weaknesses in monitoring and governance that required urgent remediation.

RBNZ and FMA set expectations for cyber risk arising from frontier AI

The Reserve Bank of New Zealand and Financial Markets Authority outlined supervisory expectations for frontier-AI cyber risk on 15 October following an industry roundtable with financial-sector leaders. The regulators said existing prudential, conduct, cyber and operational-resilience obligations already apply. Their expectations focus on increased cyber risk, evolving governance and oversight, and operational-resilience implications. They also emphasised foundational controls, third-party dependencies and clear accountability. FMA Executive Director Response and Enforcement Louise Unger said boards and senior management need to know where AI is used, understand the resulting risks and be clear about who manages them. Regulated entities should translate this into an AI service register, named risk owners, supplier assurance, access and data controls, and incident playbooks that cover model misuse, agent overreach and sudden loss of an AI-dependent process.

French refrigerator attack prompts operational-technology warning for New Zealand supermarkets

Cyberattacks targeting supermarket refrigeration systems across Europe have disrupted store operations and forced retailers to discard spoiled food after attackers remotely manipulated fridge and freezer temperatures. The incidents demonstrate how internet-connected operational technology can create direct physical and financial impacts, even when traditional corporate IT systems are not the primary target. Cybersecurity experts say the attacks should serve as a warning for New Zealand supermarkets and other organisations using connected refrigeration, building management, or industrial control systems. Businesses are being urged to review whether operational technology is unnecessarily exposed to the internet, strengthen remote access controls, apply security updates, and ensure critical systems are segmented from wider corporate networks.

NCSC urges urgent action on two critical PHP remote-code-execution vulnerabilities

New Zealand's National Cyber Security Centre issued an alert on 22 October for CVE-2026-109618 and CVE-2026-109619, two critical PHP vulnerabilities that may allow unauthenticated remote code execution. The NCSC said it was aware of reports of active exploitation and advised organisations to apply remediation urgently and investigate for unauthorised access or compromise. It also warned that PHP may be embedded in firewalls, edge devices and other platforms that require separate vendor assessment and remediation. Because PHP supports many websites, applications and APIs, an emergency response should begin with an exposure inventory rather than a generic request to patch servers. Teams should identify internet-facing instances and embedded implementations, preserve relevant web and system logs, apply vendor updates and confirm whether exploitation preceded remediation.

Australia

Unpatched server led to Victorian student data breach

An investigation into a major Victorian education data breach found that attackers exploited a critical vulnerability that had not been patched by an affected school. The attackers copied a database containing current and former student information, leading to a mass password reset shortly before the school year began. The Victorian Information Commissioner also found weaknesses in the Department of Education's guidance, vulnerability-management coverage and ability to ensure schools completed urgent remediation. Credentials belonging to former students had been retained in the same database for longer than necessary. The findings demonstrate that sending a patching instruction is not the same as confirming remediation. Central organisations should maintain visibility across distributed environments, escalate non-compliance and verify that unnecessary historical accounts and information are removed.

ATO and ASIC had earlier concerns about transcription supplier's data handling

ABC News reported on 30 October that the Australian Taxation Office and Australian Securities and Investments Commission had raised concerns in 2025 about transcription provider VIQ Solutions potentially processing sensitive information offshore. The concerns arose after the ATO received a link to a transcript available from a server in the United Kingdom. ASIC ultimately classified the matter as a near miss, but the reporting found no independent investigation across the other agencies using the provider. At least 13 government agencies had used VIQ before it was removed as an approved supplier. The case illustrates the difficulty of establishing where sensitive recordings, transcripts and court material are processed. Contracts should require disclosure of every processing location, subcontractor and support arrangement, supported by evidence rather than supplier assurances alone.

World

One operator uses AI agents to compromise more than 100 company websites

Reuters reported in October that a Chinese-speaking operator used AI agents and several thousand dollars of computing resources to compromise more than 100 company websites, including Japanese targets. The campaign is important less for a novel technique than for the economics: one person could delegate reconnaissance, testing and repetitive exploitation work to agents and operate at a scale previously associated with a larger team. Defenders should assume that internet-facing weaknesses will be discovered and exercised more quickly after publication. External attack-surface monitoring, rapid ownership of exposed assets, rate and behaviour detection, and emergency remediation therefore become incident-response controls rather than routine hygiene. Security testing teams should also preserve agent prompts, tool calls and outputs so authorised automation can be distinguished from hostile activity when a boundary is crossed.

Arizona court breach exposes information concerning 1.3 million people

An investigation into a cyberattack on Arizona's court system found that attackers copied backup files containing information relating to more than 1.3 million people. The exposed records included names, Social Security numbers and case numbers dating back approximately 30 years. Attackers also accessed more than 150,000 Foster Care Review Board reports containing information about children, families and investigations, including records concerning 8,000 children currently in foster care. Sensitive protective-order records were also copied. Investigators believe the attack began when an employee selected a malicious link in a phishing email. The breach demonstrates how backup repositories can contain broader and older information than production systems. Organisations should apply retention rules to backups, restrict and monitor access, encrypt sensitive archives and include backup data in privacy-impact and breach-notification assessments.

Ransomware attack disrupts Japanese cloud services used by 495 organisations

A ransomware attack against IDC Frontier's IDCF Cloud disrupted infrastructure used by 495 companies and local government organisations in Japan. The attack began on 7 October and forced the provider to isolate and shut down affected systems in its East Japan Region 1 data-centre cluster. Customer access to management consoles across all regions was also temporarily disabled while the provider checked whether other environments were secure. The platform supplies virtual servers, storage and networking used to operate websites, applications and business systems. The incident illustrates how a single cloud-provider compromise can simultaneously affect hundreds of customers and restrict their ability to manage their own environments. Organisations should identify which critical services depend on each cloud region, maintain recovery copies outside the affected platform and test how systems will be isolated, restored or transferred when the provider's management console is unavailable.

Summary of October'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.

- 22/10/2026 – CVE-2026-109618 and CVE-2026-109619 affecting PHP
- 2/10/2026 – CISA Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway

Our Views:

Fraud Week 2026: Cyber-Enabled Fraud Is Increasing. Is Your Organisation Ready?

International Fraud Awareness Week runs from 15 to 21 November 2026, bringing organisations around the world together to raise awareness of fraud, strengthen prevention and encourage people to recognise and report suspicious activity. This year, that message is particularly important. Fraud is increasingly enabled by technology, making it easier for offenders to reach victims, impersonate trusted people, manipulate communications and move stolen funds.

The World Economic Forum's *Global Cybersecurity Outlook 2026* found that 77% of respondents had seen an increase in cyber-enabled fraud and phishing, while 73% said they or someone in their professional or personal network had been affected by cyber-enabled fraud during 2025. Cyber-enabled fraud has also overtaken ransomware as the leading cyber concern among surveyed CEOs.

INTERPOL is seeing the same direction of travel. Its 2026 Global Financial Fraud Threat Assessment states that financial fraud has continued to increase in volume, evolve its methods and expand globally since 2024. It also highlights the growing use of artificial intelligence to support impersonation, social engineering and increasingly scalable fraud campaigns.

Fraud and cyber security can therefore no longer be treated as separate risks. An attacker may compromise an email account, but the objective is often financial. They may impersonate an executive to authorise a payment, manipulate an employee into changing supplier banking details, steal credentials to facilitate identity fraud, or use information obtained online to make a social-engineering approach more convincing. Technology provides the mechanism. Fraud provides the motive.

Awareness needs to lead to action
Fraud Week is an opportunity to remind staff about fraud risk, but awareness alone is not enough. Organisations also need mechanisms for detecting concerns early and leaders who have practised what they will do when an allegation arises. As part of our own fraud awareness initiatives, we have three practical resources available.

1. Build fraud awareness with free training

Our Fraud Risk Management course on CyberSafeHQ introduces participants to occupational fraud, why fraud occurs, common perpetrator and risk characteristics, detection and reporting, prevention, and the role individuals can play in protecting their organisation. The course is free for individual users. Organisations wanting to enrol a group of attendees can contact us to arrange organisational access and reporting. The course currently includes eight lessons and approximately 30 minutes of video content, making it an accessible way to introduce fraud risk without requiring a significant time commitment.

Access the Fraud Risk Management course

2. Give people a safe way to speak up

Employees are often one of an organisation's most effective fraud detection controls. The Association of Certified Fraud Examiners' *Occupational Fraud 2026: A Report to the Nations* analysed 2,402 occupational fraud cases across 143 countries and territories. Once again, tips were the most common way fraud was detected, accounting for 43% of cases, with more than half of those tips coming from employees. That finding has remained a consistent feature of the ACFE's research and reinforces the importance of giving employees, suppliers and other stakeholders a trusted way to raise concerns.

Our Whistleblowers service provides New Zealand organisations with an independent, confidential channel for reporting fraud, corruption, theft and other serious wrongdoing. Reports can be made through secure channels including web, email, phone and post, with anonymous reporting available.
Our Standard service starts with a $100 per month retainer, with setup and usage charges applying. It provides organisations with an independent reporting mechanism rather than expecting employees to raise sensitive allegations directly through their management structure.

Learn more about Whistleblowers

3. Practise your response before an allegation occurs

Detecting fraud is only the beginning. When an allegation is made, leaders can quickly face difficult decisions. Who needs to know? How do you protect the person who raised the concern? What evidence must be preserved? Should access to systems or funds be restricted? When should insurers, regulators, Police or other authorities become involved? Those decisions are much easier to make if they have already been practised.

Our Incident Arena solution now includes a Fraud & Corruption module designed to put leadership teams under realistic decision-making pressure. Five scenarios address key fraud risks, including:

- corruption
- expense abuse
- payroll fraud
- financial statement fraud
- money laundering

The scenarios reflect major occupational fraud categories recognised by the ACFE, including corruption, asset misappropriation and financial statement fraud.
In each scenario, the leadership team works through eight timed decisions covering issues such as protecting the person who raised the concern, securing evidence, stopping further losses and meeting reporting obligations.
Incident Arena is designed for executive and leadership teams to practise collective decision-making in a realistic but controlled environment, supported by an expert facilitator and structured debrief.

Learn more about Incident Arena or book a demonstration

Fraud resilience is a combination of people, controls and preparedness

Cyber-enabled fraud will continue to evolve. AI, compromised identities, convincing impersonation and increasingly sophisticated social engineering are making some established fraud techniques faster, cheaper and easier to scale.
The response does not need to start with more technology.

Start by ensuring your people understand the warning signs. Give them a trusted mechanism for reporting concerns. Then make sure your leadership team knows what it will do when a concern becomes a real incident.

These three capabilities can help organisations identify fraud earlier, limit its impact and respond before the damage escalates. This Fraud Week, ask three questions: Do our people recognise fraud? Can they safely report it? And are we ready to respond when they do?

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: