NZ Incident Response Bulletin

Premium Edition – June 2026 – Issue #89

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

Investing in cyber security to protect patient data

The Government announced that Budget 2026 will provide $153.6 million in funding for Health New Zealand to strengthen cyber security across the health system, including expanded national cyber security monitoring, stronger data security processes, specialist cyber security expertise, and critical IT safety upgrades. Health New Zealand is also investing an additional $300 million over the first three years of the Health Digital Investment Plan, including work to replace ageing devices, modernise radiology systems, and upgrade core IT platforms. The release specifically refers to recent incidents such as Manage My Health as evidence of the need for stronger safeguards, tighter oversight of third-party systems, annual audits of critical systems, and improved accountability for fixing cyber security risks. For executives, the key lesson is that cyber security in critical services is now being treated as a patient safety, privacy, resilience, and trust issue, not simply an IT investment.

Australia

Canvas data breach leaves education providers scrambling as student data compromised

ABC News reported on 7 May 2026 that the Canvas breach affected education providers across Australia, including state schools in Queensland and Tasmania, universities in New South Wales and South Australia, and TAFE Tasmania. Canvas is used globally by nearly 9,000 institutions, which made the incident both international and locally disruptive. The story described uncertainty among providers, students, and staff as institutions worked to understand what had been accessed and how to communicate with affected users. For executives, this is a clear example of concentration risk in education technology. A widely adopted cloud platform can become a single point of operational dependency, and a vendor breach can quickly create privacy, service continuity, legal, and reputational issues across multiple organisations. Boards should ask whether critical suppliers are mapped, whether data flows are understood, and whether cyber incident communications are ready before a supplier incident occurs.

Australia sets up Cyber Incident Review Board to learn from cyberattacks, build continuous cyber resilience

Australia has formally established a Cyber Incident Review Board to conduct no-fault reviews of significant cyber incidents and identify practical lessons for government and industry. The board sits under the Cyber Security Act 2024 and supports Australia's 2023 to 2030 Cyber Security Strategy. Its purpose is not to assign blame, but to examine major cyber events after the immediate response has concluded, identify systemic weaknesses, and recommend improvements to prevention, detection, response, and resilience. The board will be chaired by Narelle Devine, Telstra's Global Chief Information Security Officer, and includes senior leaders from academia, law, aviation, telecommunications, logistics, energy, and critical infrastructure. For executives, the development signals a maturing national approach to cyber resilience. Major incidents are increasingly being treated as learning opportunities that can improve sector-wide preparedness, supplier assurance, governance, crisis response, and operational continuity.

World

AI-related data breaches surging, Verizon report says

Reuters reported that Verizon's annual data breach report found artificial intelligence is increasingly reshaping cyber risk, with attackers using AI tools to identify software vulnerabilities, support initial access, develop malware, and accelerate attacks. The report found that exploitation of software flaws has overtaken stolen credentials as the top initial cause of data breaches for the first time, with 31% of breaches beginning through vulnerability exploitation across more than 31,000 incidents reviewed. Verizon warned that AI is shrinking the defensive response window from months to potentially hours, increasing pressure on organisations to patch and monitor faster. The report also highlighted "shadow AI", where staff use unauthorised AI tools, as a growing data-loss risk, including employees submitting source code, images, and structured data into unmanaged platforms. For executives, the key message is that AI risk is both external and internal. Organisations need faster vulnerability management, approved AI tooling, staff guidance, monitoring, and stronger integration of AI into secure development, testing, and cyber defence processes.

Google disrupts hackers using AI to exploit an unknown weakness in a company's digital defense

AP reported that Google disrupted a hacking operation in which artificial intelligence was used to help exploit an unknown software vulnerability. The report said the incident was significant because it showed AI beginning to assist cyber attackers with advanced tasks, including vulnerability identification and exploit development. Reuters separately reported that Google saw this as part of a wider shift, with criminal and state-linked actors experimenting with AI to automate and accelerate hacking operations. For executives, the business impact is that cyber risk timelines are compressing. Vulnerabilities may be discovered and weaponised faster, reducing the time available for patching and detection. Organisations should treat AI-enabled threat activity as a strategic risk, not a future issue. Priority actions include faster vulnerability management, better asset visibility, defensive use of AI, stronger logging, and rehearsed escalation when high-risk flaws emerge.

7-Eleven confirms data breach claimed by the ShinyHunters gang

BleepingComputer reported that 7-Eleven confirmed a data breach after an unauthorised third party accessed systems used to store franchisee documents. The breach, which the article said was claimed by ShinyHunters, involved access to certain documents connected to franchisee operations. For executives, the key lesson is that franchise and partner ecosystems can create significant data exposure even where consumer-facing systems are not the main target. Franchisee documents may contain personal, financial, contractual, operational, or identity information that creates legal and reputational risk if exposed. The incident also demonstrates the continued activity of ShinyHunters across high-profile organisations and sectors. Senior leaders should review where partner and franchisee information is stored, who can access it, whether documents are retained longer than necessary, and whether monitoring is strong enough to detect unusual access. Third-party and partner data should be governed with the same discipline as customer data.

Cruise operator Carnival discloses personal data breach

Carnival Corp disclosed a cybersecurity incident after an employee account was compromised in April through social engineering. The incident resulted in the exposure of some personal information, including names, addresses, and government-issued identification numbers. Carnival said it quickly blocked the unauthorised activity and engaged third-party security experts to investigate. The company is notifying affected individuals by email where possible and is offering United States customers two years of free credit monitoring through TransUnion. It has also advised affected people to monitor account activity and credit reports, stay alert for fraud, and report suspected identity theft to local authorities. For executives, the incident reinforces the business risk created by social engineering and compromised user accounts. Strong identity controls, employee awareness, phishing-resistant authentication, privileged access monitoring, and rapid containment processes are essential to reduce the likelihood and impact of similar incidents.

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.

28/05/2026 – Supply Chain Compromises Impact Nx Console and GitHub Repositories

Our Views:

Review of the 2026 Verizon DBIR: What New Zealand Organisations Need to Learn Now

Key Takeaway: The 2026 Verizon DBIR reinforces that cyber resilience still depends on disciplined execution of core controls. For New Zealand organisations, the priority is to close practical gaps in vulnerability management, third-party assurance, ransomware readiness, human risk, and AI governance, and to be able to evidence that these controls are operating effectively when boards, regulators, insurers or customers ask.

The 2026 Verizon Data Breach Investigations Report provides a timely reminder for New Zealand organisations: cyber resilience is still built on fundamentals. The report analysed more than 31,000 real-world security incidents, including more than 22,000 confirmed data breaches across 145 countries, making it the largest DBIR dataset to date. Its central message is clear. The threat landscape is changing quickly, but organisations that maintain strong asset visibility, disciplined patching, third-party oversight, incident response planning and a security-aware culture are better positioned to withstand modern attacks.

This is highly relevant in New Zealand. Recent high-profile cyber breaches have resulted in increased regulatory scrutiny and compliance notices from the Office of the Privacy Commissioner. For executives and boards, the lesson is that cyber controls are no longer simply "IT controls". They are privacy safeguards, governance controls and evidence of reasonable care.

Where personal information is involved, the ability to demonstrate reasonable security practices is critical. Organisations need to be able to show that they understand their risks, have implemented appropriate safeguards, monitor those safeguards, and can respond effectively when something goes wrong.

Key Lessons from the 2026 DBIR

The first major finding is the rise of vulnerability exploitation. The DBIR reports that exploitation of vulnerabilities is now the most common initial access vector for breaches, rising to 31%, while credential abuse fell to 13%. It also found that only 26% of CISA Known Exploited Vulnerabilities were fully remediated by organisations in 2025, down from 38% the previous year, with median full remediation time increasing to 43 days. For New Zealand organisations, this should prompt a practical review of vulnerability management. Boards should be asking whether critical internet-facing systems, cloud services, remote access platforms and third-party hosted environments are being patched based on real exploitation risk, not just generic severity scores. A vulnerability that is actively exploited should be treated as an incident waiting to happen.

The second major lesson is that ransomware remains a core business risk. The DBIR found ransomware was involved in 48% of breaches, up from 44% the previous year. However, 69% of ransomware victims in the dataset did not pay, and median ransom payments continued to decline. This does not mean ransomware is becoming less serious. It means organisations are increasingly judged on whether they can contain, recover, evidence decisions and communicate effectively under pressure.

The third major finding is the growth of third-party risk. The DBIR reports that breaches involving third parties increased by 60% from the previous year, reaching 48% of total breaches. This is a significant issue for New Zealand organisations that rely on outsourced technology providers, cloud platforms, managed service providers, software vendors and specialist business systems. Third-party outsourcing does not remove accountability. Organisations remain responsible for understanding where their data is held, who has access to it, how it is protected, and how suppliers will respond during a cyber incident. Contractual assurances are not enough. Assurance needs to be tested, evidenced and reviewed regularly.

The fourth lesson is the continuing role of people. The DBIR found the human element was present in 62% of breaches, with social engineering representing 16% of breaches. Mobile-centric vectors such as voice and text messaging produced higher success rates in simulations than email, and pretexting is becoming a more common initial access vector for ransomware and extortion attacks. This means awareness training must move beyond email phishing. Help desks, finance teams, executives, customer support teams and IT administrators need clear procedures for verifying unusual requests, resetting credentials, approving payments and granting access. Attackers are increasingly targeting process weaknesses, not just technical vulnerabilities. This is why we continue to develop and offer to our customers contextual cyber training via the CyberSafeHQ.com learning management system.

The fifth lesson is emerging AI-related data leakage. The DBIR found that 45% of employees are now regular users of AI on corporate devices, up from 15% the previous year, and that 67% of users accessing AI services on corporate devices used non-corporate accounts. It also identified Shadow AI as a rapidly growing data loss prevention issue, with source code, images, structured data and technical documentation being submitted to external AI tools. For New Zealand organisations, this requires immediate governance attention. Staff may be using AI tools to improve productivity, but without clear rules they may unintentionally expose sensitive information, personal data, source code, commercial records or internal documentation.

Why We Map These Developments to the CIS Controls

We closely follow these developments because they map to the CIS Controls for measurable risk reduction. The CIS Controls provide a practical structure for reducing the likelihood and impact of common cyber-attacks. They are especially useful because they convert threat intelligence into specific safeguards that can be implemented, tested and evidenced.

The DBIR's findings reinforce the value of using CIS Controls as a practical benchmark. Vulnerability exploitation maps to CIS Control 7, Continuous Vulnerability Management. Credential abuse and weak access governance map to CIS Controls 5 and 6, Account Management and Access Control Management. Ransomware preparedness maps to CIS Controls 11 and 17, Data Recovery and Incident Response Management. Social engineering maps to CIS Control 14, Security Awareness and Skills Training. Third-party exposure maps to CIS Control 15, Service Provider Management. Shadow AI and data leakage map to CIS Controls 3 and 8, Data Protection and Audit Log Management.

The practical value is that the CIS Controls help organisations ask the right questions:

- Do we have this safeguard?
- Is it operating effectively?
- Can we produce evidence?
- Has it been tested during a realistic incident scenario?

Those questions are increasingly important when regulators, insurers, auditors, customers and boards assess whether an organisation acted reasonably.

What New Zealand Organisations Should Do Next

New Zealand organisations should treat the DBIR as a board-level risk input, not simply a technical report. In light of recent high-profile breaches and compliance action from the Office of the Privacy Commissioner, organisations holding personal or sensitive information should review whether their security controls can be evidenced, not just described.

Priority actions should include:

- Confirm complete visibility of internet-facing assets, cloud services, privileged accounts and third-party data stores.
- Review vulnerability management against active exploitation, especially for externally exposed systems.
- Enforce MFA for remote access, privileged users, externally exposed applications and third-party platforms.
- Test incident response plans through realistic executive tabletop exercises, including privacy notification, regulator engagement, media response, ransomware decision-making and business continuity.
- Review third-party contracts, assurance processes and security evidence, particularly where suppliers host or process personal information.
- Establish clear AI usage rules, including approved tools, account requirements, data restrictions and monitoring for unauthorised use.
- Align cyber and privacy governance so that security weaknesses are assessed in terms of potential privacy harm, not only technical impact.

The strongest message from the 2026 DBIR is that cyber risk reduction is still achieved through disciplined execution of known controls. For New Zealand organisations, the regulatory context makes this more urgent. Where personal information is involved, weak cyber hygiene can quickly become a privacy compliance issue, a governance issue and a public trust issue.

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: