NZ Incident Response Bulletin

Standard Edition – April 2025 – Issue #75

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

NZ businesses complacent over cyber security threats – report

A survey by Datacom revealed a concerning complacency among New Zealand businesses regarding cybersecurity. While 71% of business leaders believed their staff were well-prepared for cyber threats, only 51% of employees concurred. This overconfidence leaves organizations vulnerable to increasingly sophisticated attacks, particularly those utilizing artificial intelligence. Datacom's Chief Information Security Officer, Collin Penman, highlighted the disparity between perceived and actual preparedness, stressing the urgency for businesses to embed robust cybersecurity governance and invest in resilience strategies to mitigate evolving threats.

The cost of cyber crime: 91 percent increase in 12 months

According to data released in March 2025 by CERT NZ, the financial impact of cybercrime in New Zealand surged by 91% over the past year, reaching $39 million in direct losses. The report highlights a sharp rise in phishing attacks, online scams, and business email compromise incidents. Notably, small and medium-sized businesses have become more frequent targets, with many lacking adequate cybersecurity defenses. CERT NZ emphasized that the sophistication of cybercriminals is increasing, often involving well-crafted social engineering tactics and the use of emerging technologies like AI to deceive victims. The agency urged organizations to adopt multi-factor authentication, conduct regular staff training, and maintain strong incident response plans. This escalation in cybercrime underscores the urgent need for both the private and public sectors to strengthen their cyber resilience against an evolving threat landscape.

Spy agency minister Judith Collins refuses to release Pacific cyber security documents

New Zealand's Minister for the Intelligence Agencies, Judith Collins, declined to release classified documents detailing New Zealand's cyber security initiatives in the Pacific region. The refusal came amid growing concerns over regional cyber threats and foreign interference, particularly from state actors. Collins cited national security concerns and the protection of intelligence sources and methods as reasons for withholding the documents. Critics argue that greater transparency is needed, especially as Pacific nations face increasing cyber risks and infrastructure vulnerabilities. However, Collins stressed that while the government supports strengthening cyber resilience across the Pacific, it must also safeguard sensitive operational details.

New Database Improves Effort to Stop Terrorist and Violent Extremist Material

the New Zealand government announced the launch of a new digital database designed to strengthen efforts to detect and block terrorist and violent extremist content online. Developed through a partnership between the Department of Internal Affairs and international counterparts, the database consolidates information about known harmful material, enabling faster identification and removal across digital platforms. This initiative aligns with New Zealand's commitment under the Christchurch Call to Action, a global movement to eliminate terrorist and violent extremist content online. Officials emphasized that the database enhances real-time threat monitoring and supports digital service providers in swiftly responding to harmful uploads. Privacy and human rights safeguards have been built into the system to ensure its use remains targeted and proportional. This development marks a significant step in enhancing national and international cyber resilience against extremist threats in the digital space.

Australia

Australia regulator sues FIIG Securities for cybersecurity failures

The Australian Securities and Investments Commission (ASIC) filed a lawsuit against FIIG Securities, accusing the firm of failing to adequately protect sensitive customer data from cybersecurity threats. The regulator alleges that FIIG did not implement sufficient cybersecurity controls between 2014 and 2020, exposing client information to significant risk. This case marks a major move by ASIC to hold companies accountable under Australia's new, tougher cybersecurity enforcement regime. ASIC contends that FIIG's prolonged weaknesses, including poor risk management and inadequate breach detection capabilities, reflect systemic governance failures. Although this lawsuit originates in Australia, it carries important implications for New Zealand firms operating trans-Tasman, as it highlights rising regulatory expectations for cybersecurity resilience and proactive data protection across the region. Organizations are urged to treat cybersecurity not just as an IT issue, but as a board-level governance and compliance priority.

Poorly funded hospitals risk more cyber attacks

Cybersecurity experts warned that the recent ransomware attack on a major Australian IVF clinic could signal a growing trend of cybercriminals targeting sensitive healthcare and fertility services. The attack, which compromised highly personal patient data, highlighted the vulnerabilities within private healthcare providers, many of which lack the robust cybersecurity infrastructure of larger hospital systems. A leading US cybersecurity group cautioned that threat actors are increasingly drawn to industries where data sensitivity is high and the pressure to pay ransoms is acute. Analysts emphasized that the healthcare sector must urgently adopt stronger cybersecurity controls, including advanced encryption, network segmentation, and incident response planning. The incident also prompted renewed calls for mandatory breach disclosure laws in Australia and New Zealand, to ensure timely reporting and coordinated responses to cyberattacks involving critical personal health information.

Hacker claims Oracle breach, sending business and agencies scrambling

A hacker group claimed responsibility for breaching Oracle's cloud infrastructure, sparking urgent investigations across businesses and government agencies that rely heavily on Oracle's services. Although Oracle initially reported limited disruption, security experts warned that the attackers might have accessed sensitive enterprise data, potentially affecting thousands of customers globally. The breach particularly alarmed financial services, healthcare providers, and government departments, sectors that depend on Oracle's cloud and database solutions. Cybersecurity firms advised affected organizations to immediately review access logs, strengthen credentials, and apply available patches. Oracle stated that it was working closely with law enforcement and external investigators but has not publicly confirmed the extent of the breach. This incident underscores the growing risks posed by supply chain attacks on major technology providers and the need for organizations to maintain layered defenses even when using trusted third-party platforms.

World

Elon Musk says X target of 'massive cyberattack'

In March 2025, Elon Musk revealed that his social media platform X (formerly Twitter) was the target of a "massive" and highly coordinated cyberattack. Musk did not specify who was behind the attack but suggested that it was sophisticated and likely state-sponsored. Although the platform experienced some disruption, Musk confirmed that no significant data breaches had occurred, and user information remained secure. He emphasized that the attack aimed to destabilize X's services rather than steal user data. The incident raised concerns about the growing vulnerability of major communication platforms to cyber threats, especially as X has been positioning itself as a central hub for financial transactions and news distribution. Cybersecurity experts warned that platforms like X, which hold vast volumes of sensitive user data and financial information, are increasingly attractive targets for sophisticated cyber operations.

Google makes its biggest-ever acquisition

In March 2025, Google announced its largest acquisition to date, purchasing cybersecurity firm Mandiant for US$18 billion. The move underscores Google's strategic focus on bolstering its cloud services security offerings amid rising global cyber threats. Mandiant, renowned for its threat intelligence and incident response capabilities, will enhance Google's ability to provide proactive cybersecurity solutions to corporate and government clients. Analysts view the acquisition as a direct response to intensifying competition from Microsoft and Amazon in the cloud security space. Google executives emphasized that integrating Mandiant's expertise will enable faster threat detection, stronger defense mechanisms, and improved customer trust. This acquisition reflects a broader industry trend where tech giants are rapidly expanding their cybersecurity portfolios to meet escalating demand for robust and integrated digital protection services.

Officials warn against dangerous Medusa ransomware attacks. Here's how to stay protected.

U.S. federal officials issued urgent warnings about a surge in cyberattacks linked to the "Medusa" ransomware gang, which has increasingly targeted schools, hospitals, and local governments. Medusa's tactics involve encrypting critical systems and threatening to leak stolen data unless large ransoms are paid, often demanding millions of dollars. Authorities report that the group's attacks have become more sophisticated, using stealthy methods to evade detection and prolong network access before launching ransomware payloads. Victims include multiple educational institutions and regional healthcare providers, causing widespread service disruptions. Officials stressed the importance of immediate defensive actions such as applying patches, enforcing strong access controls, and maintaining up-to-date offline backups. The resurgence of Medusa highlights the escalating threat ransomware poses to public sector entities and the urgent need for comprehensive cybersecurity strategies across vulnerable infrastructure sectors.

US charges Chinese nationals in cyberattacks on Treasury, dissidents and more

The U.S. Department of Justice announced charges against seven Chinese nationals allegedly linked to a series of cyberattacks that compromised multiple U.S. government agencies, including the Department of the Treasury. The individuals, believed to be associated with a Chinese state-sponsored hacking group, were accused of conducting extensive espionage operations over several years. Prosecutors outlined how the hackers used sophisticated spear-phishing campaigns and malware to infiltrate networks and exfiltrate sensitive information related to economic policy, defense strategies, and diplomatic communications. Although the indictments are largely symbolic, given the low likelihood of extradition, U.S. officials emphasized that the action is intended to deter future state-backed cyber operations and to signal international condemnation. The case underscores the persistent threat posed by advanced persistent threat (APT) groups and the need for continuous vigilance in protecting critical government and financial systems worldwide.

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.

12/03/2025 – CISA and Partners Release Cybersecurity Advisory on Medusa Ransomware

Our Views:

Why Cyber Simulations Matter More Than Ever - for Executives, Too

From the field, we see it time and time again. A company gets hit with a cyberattack and their data is encrypted, systems go down, and panic sets in. It's not just IT scrambling when this happens. The legal team is fielding compliance questions, communications is trying to craft a statement while email is offline and finance are looking to ensure critical transactions can progress. The executive team starts to ask the right questions - but for many, it's the first time they've had to ask them at all.

Cyber simulations are one of the most valuable tools we have to prevent that scenario from spiralling out of control.

In responding to hundreds of cyber incidents across New Zealand, we see a clear pattern: the organisations that fare best are not the ones with the most expensive software or the largest IT teams. They're the ones where leaders have rehearsed what a real incident feels like. Where decisions have been tested under pressure. Where cyber resilience isn't just a policy - it's muscle memory.

Business continuity plans (BCP) used to primarily focus on natural disasters, power outages, and maybe a fire. Today, however, it is ransomware, business email compromise, third-party outages, and data leaks that frequently require an effective crisis response. These digital threats hit hard, spread fast, and they impact the entire organisation.

While having a BCP is a foundational step, its true value lies in how well it performs under pressure - making regular testing essential. That is why cyber simulations now sit at the heart of modern business continuity.

Cyber simulations are not just technical drills. They are full-scale exercises that draw in executives, legal, communications, finance, and yes, your IT and security teams too. Because when an incident hits, the entire business needs to know how to respond—not just the people in the server room.

One area that's often overlooked in these exercises is your third-party technology providers. That includes those that supply and manage your cloud platforms, payroll systems, legal technology and more - the backbone of day-to-day operations. These vendors are deeply integrated into your workflows but rarely tested in incident scenarios. From our perspective, this is a major blind spot. Some of the most difficult responses we've managed involved vendors who couldn't - or wouldn't - communicate quickly or who didn't have a viable recovery plan of their own. When your systems go down because a supplier is under attack, their crisis becomes yours. That's why it's essential to pull them into your simulations, or at the very least, ask them hard questions about their own readiness and response processes.

Cyber simulations expose important gaps before they become headlines. They show where assumptions break down, where delays creep in, and where critical decisions need clearer ownership. Most importantly, they give executive teams a real-world feel for what a cyber crisis looks like - and how fast it moves.

We see firsthand the difference regular cyber simulation exercises make. When a board has been through a realistic cyber scenario, they respond with focus. They ask the right questions, they trust the process, and they support the response rather than unintentionally slow it down.

The ability to bounce back from a cyber-attack hinges on how well an organisation can execute its business continuity strategy. Simulation-based testing transforms a theoretical plan into a practiced, coordinated response. This not only builds confidence across the organisation but significantly increases the chances of maintaining operations and recovering quickly during a real cyber incident.

In short, regularly testing business continuity through realistic exercises isn't just good practice, it's a critical investment in your organisation's resilience. Digital disruption isn't a risk - it's a reality. Practicing under pressure is what builds resilience. Not after an attack - but before it. That's the work that matters.

If your executive team hasn't practiced a cyber incident response, start now. Even a two-hour tabletop exercise can reveal critical gaps - and build the confidence needed to lead through a crisis.

Finally, recent updates to our feedback reporting tool now include a gaps analysis against the New Zealand National Cyber Security Centre's Incident Management guidelines, and the Coordinated Incident Management System (CIMS). Contact us to learn more about how a cyber simulation can help your organisation be better prepared.

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: