# NZ Incident Response Bulletin

## Standard Edition – March 2024 – Issue #62

*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.*

Not subscribed to our Premium Bulletin? Click here to join.

## 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 police among agencies in cybercrime takedown of LockBit ransomware group

New Zealand police, in collaboration with international law enforcement agencies, achieved a significant breakthrough in the fight against cybercrime. Led by the United Kingdom's National Crime Agency (NCA), the operation infiltrated the notorious LockBit ransomware group, disrupting their activities. LockBit had been operating for four years, launching prolific ransomware attacks globally, including in the UK. The group provided "ransomware-as-a-service" to a network of hackers, supplying tools and infrastructure for attacks. The NCA seized LockBit's administration environment, leak site on the dark web, and obtained their source code. Two defendants responsible for LockBit attacks are now charged and in custody, with further indictments against Russian nationals. The operation spanned ten countries, including the FBI and Australian Federal Police, with New Zealand Police playing a crucial role.

Minister warned to protect critical infrastructure amidst increasing risk

New Zealand's critical infrastructure faces mounting risks, and officials have stressed the urgent need to safeguard essential systems such as water treatment plants. In their briefing to Prime Minister Christopher Luxon, they highlighted the threat of foreign interference, particularly attempts to co-opt influential individuals. The briefing comes amidst major national security reforms following the 2019 mosque attacks. A strategic focus on countering foreign interference aims to enhance resilience, but legislation is still pending.

New Zealand signs up to alliance targeting hackers-for-hire

New Zealand has joined an international alliance aimed at countering hackers-for-hire. The so-called Pall Mall process, signed by 34 countries during an inaugural conference in the UK, seeks to reduce the commercial market for malicious spyware. While New Zealand's participation does not impose specific obligations, it underscores the importance of public-private collaboration in securing a free and secure cyberspace. The country already employs a range of measures to tackle threats from malicious cyber activity.

### Australia

What companies can learn from HWL Ebsworth hack

Australian law firm HWL Ebsworth fell victim to a Russian-linked ransomware attack in April, resulting in the exposure of sensitive information. The hackers, part of the ALPHV/Blackcat group, claimed to have stolen 4TB of company data, including employee CVs, IDs, financial reports, accounting data, client documentation, credit card information, and a complete network map. The breach affected numerous clients, including government agencies, and raised concerns about cybersecurity vulnerabilities and the need for robust defences.

Chinese embassy confronts Australian cyber ambassador who accused Beijing of cyber attacks

A Chinese embassy official confronted Australia's new cyber ambassador after he told a gathering of diplomats in Canberra that Beijing was responsible for a series of devastating online attacks against the country. During a briefing on Australia's new Cyber Security Strategy, the ambassador for cyber affairs and critical technology, Brendan Dowling, highlighted how Australia had publicly attributed several online attacks to China, as well as Russia, Iran, and North Korea. The Chinese representative disputed Australia's assessment, asserting that China is a positive force globally and wants to "work constructively with other nations" on cyber matters. The incident underscores the ongoing tensions between Australia and China regarding cybersecurity issues.

Michelle McGuinness appointed national cyber security coordinator

Lieutenant General Michelle McGuinness has been appointed as the new National Cyber Security Coordinator by the Department of Home Affairs in Australia. Replacing Air Commander Australia Darren Goldie, who was recalled after four months, McGuinness brings her military intelligence expertise to the role. Her mission is to protect against and respond to major cyber security threats and incidents facing Australia. The appointment underscores the importance of public-private collaboration in securing a free and secure cyberspace. The National Office of Cyber Security (NOCS), launched last year, will play a crucial role in synchronizing Commonwealth agencies' responses and protections against cyber incidents.

## World

Nation-state actor used stolen Okta credentials in Thanksgiving attack, Cloudflare says

In a Thanksgiving Day attack, a suspected nation-state actor breached Cloudflare's systems using credentials stolen from Okta. The attacker gained access to internal systems, including the company's wiki and bug database. They also infiltrated Cloudflare's source code management system. The stolen credentials were from a widely-publicized October breach at Okta. Although the impact was limited, Cloudflare took the incident seriously, suspecting the attacker aimed to obtain persistent and widespread access to their global network. The company swiftly rotated production credentials and secured their network against future threats.

New ScreenConnect RCE flaw exploited in ransomware attacks

Cybercriminals are exploiting a critical authentication bypass vulnerability in ScreenConnect, a popular remote access tool. By breaching unpatched ScreenConnect servers, they deploy LockBit ransomware on compromised networks. Despite recent law enforcement takedown efforts, LockBit attacks continue, with threat actors leveraging these vulnerabilities. The situation underscores the urgency of patching and securing remote access tools to prevent further ransomware incidents.

AnyDesk Hit by Cyber-Attack and Customer Data Breach

AnyDesk, a widely used remote desktop software provider, confirmed that its production systems were compromised in a recent cyber-attack. Adversaries stole source code and private code signing keys, gaining access to the firm's production systems. The company swiftly activated a remediation plan with the help of cybersecurity experts from CrowdStrike. Although the hack did not impact end-user devices, AnyDesk has revoked all security-related certificates and web portal passwords. Additionally, compromised AnyDesk login credentials are being sold on both the clear and dark web by multiple threat actors. The situation is now under control, and users are advised to use the latest version and change passwords if needed.

International Cybercrime Malware Service Dismantled by Federal Authorities: Key Malware Sales and Support Actors in Malta and Nigeria Charged in Federal Indictments

Federal authorities in Boston have seized internet domains used by cybercriminals to sell computer malware, including the sophisticated Warzone RAT. This remote access trojan allowed cybercriminals to secretly connect to victims' computers, steal data, and engage in other malicious activities without the victims' knowledge. Additionally, indictments were unsealed against individuals in Malta and Nigeria involved in selling the malware and supporting cybercriminals. The operation involved global cooperation and underscores efforts to combat cyber threats worldwide.

Cyber-attacks by North Korea raked in $3bn to build nuclear weapons, UN monitors suspect

UN sanctions monitors are currently investigating 58 suspected cyber-attacks carried out by North Korea between 2017 and 2023. These attacks, valued at approximately $3 billion, are believed to have helped fund North Korea's nuclear weapons development. The country's hacking groups, operating under its primary foreign intelligence agency, continued their high number of cyber-attacks. Despite UN sanctions, North Korea has further developed nuclear weapons and produced nuclear fissile materials. The report highlights the ongoing challenge of combating cyber threats and enforcing sanctions.

US pharmacy outage triggered by 'Blackcat' ransomware at UnitedHealth unit, sources say

Change Healthcare, a health care technology company owned by UnitedHealth Group, has been grappling with a cyberattack that began on February 21. The attack disrupted several of its systems and services, prompting the company to disconnect its systems in the interest of protecting partners and patients. Due to its widespread presence and critical services, this interruption could significantly impact the health care field, affecting revenue cycles, pharmacy services, clinical authorizations, and more. While Change Healthcare has not provided a specific recovery timeframe, it has expressed confidence that Optum, UnitedHealthcare, and UnitedHealth Group systems remain unaffected. However, health care organisations are advised to independently evaluate information provided by Change Healthcare and consider the potential business and clinical disruptions when reconnecting to nonimpacted systems.

Southern Water customers affected by cyber attack

Southern Water, a company providing water services across Kent, Sussex, Hampshire, and the Isle of Wight, has reported a cyber attack in which data belonging to 5-10% of its customers was stolen. The stolen data includes personal details such as names, dates of birth, national insurance numbers, bank account details, and reference numbers. The company has been monitoring suspicious activity in its IT systems and is notifying affected customers. While services and water supplies remain unaffected, the Information Commissioner's Office (ICO) is investigating the incident.

## 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.

9/02/2024 – Fortinet Releases Security Advisories for FortiOS

29/02/2024 – Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

## Our Views:

### The NIST Cybersecurity Framework (CSF) 2.0

The National Institute of Standards and Technology (NIST) has released an updated version of its cybersecurity framework (CSF). We think this version offers significant improvements over the previous versions by widening its scope, supplying more support tools for implementation, and focusing more heavily on cyber governance activities which are critical for cybersecurity success.

Following a presidential Executive Order, NIST first released the CSF in 2014 to help organisations understand, reduce and communicate about cybersecurity risk.

According to NIST, *"The new edition is designed for all audiences, industry sectors and organisation types, from the smallest schools and nonprofits to the largest agencies and corporations — regardless of their degree of cybersecurity sophistication. In response to the numerous comments received on the draft version, NIST has expanded the CSF's core guidance and developed related resources to help users get the most out of the framework. These resources are designed to provide different audiences with tailored pathways into the CSF and make the framework easier to put into action."*

We consider that the NIST CSF is a useful governance tool in assisting with managing cyber risk from a high level, however it should not be considered the only one. We also recommend adopting other governance tools to work alongside NIST CSF, primarily the Centre for Internet Security (CIS) Controls. Fortunately, the two can be largely mapped to each other to avoid double handling.

An outline of the key changes to the framework and links to the additional support tools is given below.

**Expanded Scope**

Recognising that cyber threats now impact all industries and all organisations regardless of size, the NIST CSF, originally titled "Framework for Improving Critical Infrastructure" has been adapted and made useful for all sectors. The framework now explicitly aims to assist all organisations in their cybersecurity goals, including those with limited resources or low baseline maturity. This is a positive change and makes the NIST CSF more accessible and relevant to New Zealand organisations.

**New GOVERN function**

In addition to the existing core framework functions of IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER, a function that focuses on cyber governance activity is now included which firmly embeds cybersecurity improvements into the wider business context. We welcome the introduction of the GOVERN Function in this version of the framework as we see cyber governance as being an area requiring greater attention from New Zealand organisations to enable successful cyber programmes.

The NIST CSF governance function reinforces how cybersecurity is a major source of business risk that must be considered by senior leadership as part of the overall business risk process. It achieves this by providing steps to prioritise and implement the other five core function activities in the context of an organisations overall mission and stakeholder expectations. The Govern function also incorporates steps to manage an increasingly concerning area of cyber risk: cybersecurity supply chain risk management. The Govern function ensures the organisation's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored via six categories as outlined below:

- Organisational Context: *The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organisation's cybersecurity risk management decisions are understood.*
- Risk Management Strategy: *The organisation's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.*
- Roles, Responsibilities and Authorities: *Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.*
- Policy: *Organisational cybersecurity policy is established, communicated, and enforced.*
- Oversight: *Results of organisation-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.*
- Cybersecurity Supply Chain Risk Management: *Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organisational stakeholders.*

The NIST CSF Tiers now also include a sliding category to characterise the rigor of an organisation's cybersecurity risk governance practices (GOVERN) as well as the cybersecurity risk management practices (IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER). The categories range from Tier 1, which indicates partial risk governance where the application and prioritisation of cybersecurity risk is ad hoc, through to Tier 4, which indicates adaptive risk governance using an organisational-wide approach.

**Additional Support Resources**

The NIST CSF support resources have also been expanded to include new quick start guides, informative references, implementation examples, and a repository of organisational profiles that will be updated continuously by NIST. These additional resources are intended to offer different organisations and industries tailored pathways to implementing the framework and lifting their cybersecurity maturity. The resources can be customised and used in combination to suit various organisational contexts and capabilities. Additional frameworks and guidance documents are also being evolved that sit alongside the CSF and attempt to address emerging technology issues relevant to 2024, such as the AI Risk Management Framework and the Cybersecurity Supply Chain Risk Management Practices for Systems and Organisations.

An example of the available implementation guidance for a subset of one category in the new govern function is demonstrated below:

| Function | Category | Subcategory | Implementation Example |
|---|---|---|---|
| GOVERN (GV) | Organisational Context (GV.OC) | GV.OC-01: The organisational mission is understood and informs cybersecurity risk management | Share the organisation's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission |

Managing the ever-expanding cyber risk landscape must be a continuous process. The updated NIST CSF now offers an even more comprehensive view of cyber risk management for organisations, and we recommend reviewing the new GOVERN function and support resources to assess applicability and usability for your business.

## 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: