NZ Incident Response Bulletin

Standard Edition – September 2023 – Issue #56

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

The Front Page: Do police need to rethink their approach to scams, cyber fraud?

For years, the joke around cyber fraud and online scams has always been that of an African prince emailing to say you've won millions, if you only fill out this form. But as artificial intelligence gets more sophisticated, and the groups running these scams get bigger and more organised, the risk of cyber fraud hitting your pocket is growing by the day - and the police seem ill-equipped to deal with it. University of Canterbury sociologist and director of Independent Research Solutions, Dr Jarrod Gilbert, wrote for the Herald earlier this week on the growing number of Kiwis being impacted by cyber fraud. A recent Crime and Victims Survey showed that 510,000 New Zealanders had been victims of fraud and deception over the last 12 months.

Out of the shadows: Why making NZ's security threat assessment public for the first time is the right move

Opinion - Friday's release of the threat assessment by the New Zealand Security Intelligence Service (SIS) is the final piece in a defence and security puzzle that marks a genuine shift towards more open and public discussion of these crucial policy areas. Together with July's strategic foreign policy assessment from the Ministry of Foreign Affairs, and the national security strategy released last week, it rounds out the picture of New Zealand's place in a fast-evolving geopolitical landscape. From increased strategic competition between countries, to declining social trust within them, as well as rapid technological change, the overall message is clear: Business as usual is no longer an option. By releasing the strategy documents in this way, the government and its various agencies clearly hope to win public consent and support - ultimately, the greatest asset any country possesses to defend itself.

Rise in scams & fraud: How are banks responding?

Nine to Noon looked at the issue of online fraud and whether banks could - and should - be doing more to protect customers' losses. Kathryn spoke with Jon Duffy from Consumer NZ about whether the New Zealand Code of Banking Practice was robust enough to protect Kiwi bank users, and anti-scam consultant Bronwyn Groot about the increasing sophistication of scammers. Millions are being stolen from Kiwis each year - likely a gross underestimate of the true situation because many victims feel embarrassed and don't report their losses. Nine to Noon has been seeking a discussion with the heads of the major banks in New Zealand to talk about the rise of online scams and how they're dealt with. Only one agreed. This morning Kathryn speaks with ANZ's CEO Antonia Watson.

Cybersecurity: Growing government reliance on offshore cloud services has security experts worried

A China-linked hack of US government cloud email accounts is raising questions about the New Zealand Government's growing reliance on American data firms. A small but growing number of government tenders here specify a preference for Microsoft or Amazon Web Services (AWS) systems, products or services. Only those two US firms have special memorandum of understanding (MOU) deals with the Government, and ministers have all but ordered all their agencies to use such off-site cloud computing from private firms. In the US, officials and Microsoft recently revealed that hackers secretly accessed email accounts at two dozen organisations, including at least two US government agencies. The New York Times quoted a "person briefed on the intrusion" saying "the attack showed a significant cybersecurity gap in Microsoft's defences and raised serious questions about the security of cloud computing". Microsoft was one of the New Zealand Government's two go-to cloud providers, the other was Amazon.

World

Russia Tipped As Prime Suspect Over Huge Cyber Attack On UK Electoral Commission

Russia is believed to be behind a cyber attack on the UK's Electoral Commission which saw the data of 40 million voters exposed for two years. The attack was discovered in October last year after suspicious activity was detected, and it was realized that the attackers had first gained access in August 2021. "We regret that sufficient protections were not in place to prevent this cyber-attack," says Electoral Commission chief executive Shaun McNally. "Since identifying it we have taken significant steps, with the support of specialists, to improve the security, resilience, and reliability of our IT systems." The hackers were able to access reference copies of the electoral registers, held by the Commission for research purposes and to carry out permissibility checks on political donations. This data included the name and address of all those in the UK who were registered to vote between 2014 and 2022, as well as the names of those registered as overseas voters. The Commission's email system was also accessible during the attack.

AWS pledges $20M to K-12 cyber training, incident response

Amazon Web Services committed $20 million for a grant program to support cyber resilience, as rival technology firms and school administrators are scheduled to meet at the White House to roll out a broad effort to prevent ransomware and other malicious threat activity from harming K-12 schools. AWS said the funding will go toward cloud-based cybersecurity programs for K-12 school districts and state departments of education. The company is participating in a larger collaboration between government agencies and private sector partners to help resource poor organizations like local schools combat malicious attacks.

Cyber-attack to cost outsourcing firm Capita up to £25m

Capita expects to take a financial hit of as much as £25m as a result of a cyber-attack that began in March, pushing the outsourcing group to a pre-tax loss of almost £68m for the first half of the year. The group is still recovering from the attack by the Black Basta ransomware group, which hacked its Microsoft Office 365 software and accessed the personal data of staff working for the company and dozens of clients. Capita confirmed on Friday that "some data was exfiltrated" from its IT systems but added that this was less than 0.1% of its server estate. The company added: "That data has been recovered and extensive steps have been taken to secure the data. Impacted customers, suppliers and employees have now been contacted and we are supporting those whose data was exfiltrated."

Cyber-Attack on Australian Utility Firm Energy One Spreads to UK Systems

A cyber-attack on Australian utility company, Energy One Limited (EOL), could have international impact with the firm's corporate systems in the UK also affected. The company, a global supplier of software and services to the wholesale energy market, confirmed that it had taken steps to limit the impact of the incident and had alerted both the Australian Cyber Security Centre and "certain UK authorities." According to a document signed by Andrew Bonwick, Board Chairman of EOL, it was established that the firm's corporate systems had been affected on August 18, 2023. The statement was made on August 21 and published on the Australian Securities Exchange website (ASX).

Japan's cyber security agency suffers months-long breach

The organisation responsible for Japan's national defences against cyber attacks has itself been infiltrated by hackers, who may have gained access to sensitive data for as much as nine months. According to three government and private sector sources familiar with the situation, Chinese state-backed hackers were believed to be behind the attack on Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), which began last autumn and was not detected until June. The discovery of the incident and the sensitivity of the target comes at a time of unprecedented scrutiny of Japan's vulnerability to cyber attack. Tokyo is embarking on deeper military co-operation with the US and regional allies, including work on a joint fighter project with the UK and Italy, in which top secret technological data will be exchanged.

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.

16/08/2023 – CISA Releases JCDC Remote Monitoring and Management (RMM) Cyber Defense Plan

4/08/2023 – CISA Releases its Cybersecurity Strategic Plan

3/08/2023 – 2022 Top Routinely Exploited Vulnerabilities

Our Views:

Cyber risks associated with the supply chain

Information technology product and service suppliers are essential to the smooth operation of most organisations in New Zealand today. However, service providers are also often the unknown piece of the security puzzle when it comes to ensuring your organisation and its critical data and resources are protected from cyber incidents. Visibility into the security measures and practices of the development, delivery and operational lifecycles of many service providers is often low. However, this is changing as more focus is being placed on the potential vulnerabilities in the supply chain due to targeted attacks in this area. The IT supply chain may be exploited through hardware, software or through service providers and these risks can be present for various reasons for example:

- Suppliers may not adequately protect their own systems leading to vulnerabilities that can be exploited to the detriment of their customers. This can occur due to financial pressures, unskilled resources or sheer negligence and mismanagement.
- Suppliers may have a malicious employee acting on the inside to cause harm to them and either intentionally or as a byproduct, harm to their customers.
- Suppliers may act purely for their own interests. For example, by failing to upgrade or update systems, by stealing or sharing intellectual property or leaving a customer open to attack.
- Organisations may not clearly articulate their security requirements or disclose the criticality of their data or systems, leading to a supplier failing to notify of relevant threats.
- Shadow IT procurement may introduce products or services into your business that have not gone through adequate due diligence.

Managing supply chain risks involves challenges. Many suppliers may contribute to the production, supply and service of a single product making transparency almost impossible to achieve. Determining the likelihood and possible severity of these risks is also challenging as many risks involve actions that are hard to predict, such as the likelihood of contractor turnover at any one vendor. Additionally, some suppliers may impose visibility restrictions on operations to maintain proprietary products or processes.

Despite rising supply chain incidents, there is a currently a distinct lack of robust processes in place to manage these risks globally as the world becomes ever more interconnected. IT supply chains are inherently difficult to secure which means you will always have some element of unknown risk. However, there are risks that can be identified and managed through supply chain security and structured management.

All known risks should be catalogued and addressed through a process of Identification, Assessment, Mitigation and Monitoring. There are many reputable resources available to assist in ensuring you employ a structured process including the following:

- https://www.ncsc.govt.nz/resources/cyber-resilience-guidance/supply-chain
- https://protectivesecurity.govt.nz//assets/Governance/4a55e18043/Assessing-your-supply-chain-security.pdf
- CIS Critical Security Controls (cisecurity.org)
- SCRM Essentials: Information and Communications Technology Supply Chain Risk Management (SCRM) in a Connected World (cisa.gov)

To protect against the unknown risks you must build strong, layered defences around your most critical assets. Additional steps such as building awareness of the potential risks in the supply chain, understanding and being very transparent about your organisation's risk appetite, and enabling employees to address risk promptly should also be considered.

The NCSC suggests organisations consider how every supply chain could potentially contain a trojan horse and we also believe being aware and acting where possible to minimise these growing risks is vital.

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: