NZ Incident Response Bulletin

Standard Edition – June 2023 – Issue #53

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

Reserve Bank finally says it did 'not pay ransom'

The Reserve Bank has finally confirmed, more than two years after first being asked and six months into an ongoing Ombudsman's investigation, that it did not pay a ransom after it was hacked in 2020. A large amount of information supplied to the Reserve Bank by commercial banks was compromised in 2020, after hackers discovered a security hole in a commercial software system, called Accellion, which the central bank used to receive information. Up until recently, the Reserve Bank had declined to say whether it had paid off the hackers to dissuade them from dumping the stolen information online.

Privacy a vital tool for small businesses – now and into the future

Building privacy into your organisation not only means you meet your obligations under the Privacy Act 2020, but also builds trust with your customers - that's the message from the Office of the Privacy Commissioner's (OPC) latest Insights Report.
At the end of 2022, the Office of the Privacy Commissioner (OPC) and business.govt.nz ran a Small Business Privacy Awareness Survey and 386 small businesses responded. The Office also reviewed 1,487 breach reports to the Office to draw insights about small businesses and privacy. The Small Business insights report is available on the Office of the Privacy Commissioner website.

Privacy breaches, whether caused through a malicious act, human error, or system malfunction, work to erode trust in businesses, and cause the business to miss out on growth and new customers. Privacy Commissioner, Michael Webster said, "While businesses showed they understood personal information and privacy issues they didn't always have relevant privacy policies and procedures in place." "We identified four key insights from our work and explored those with the aim of helping small businesses better meet their obligations under the Privacy Act 2020."

The Government's latest budget increases the money made available to ward off cyber attacks against critical national infrastructure

The Government is increasing funding to protect vital infrastructure from cyber attacks. Extra money was unveiled in last week's budget for this purpose. The money will go to a sub branch of the Government Communications Security Bureau (GCSB). It is the National Cyber Security Centre (NCSC), and its extra funding is going up by $1.7 million, $2.0m, $2.7m and again, $2.7m, over four years. This is on top of the NCSC's existing expenditure. That money comes out of the total budget for the GCSB, which at $234m is eight times what it was 20 years ago. In its statement, the Budget says the extra money will pay for "technical advice and engagement to improve the cyber resilience of critical national infrastructure." The statement does not say what the infrastructure is, but comments over several years have listed several key installations, such as police national headquarters and the control room at Transpower that runs the national electricity system.

New Zealand, Five Eyes issue alert warning of China state actor engaging in 'malicious cyber activity'

Five Eyes intelligence agencies have issued an alert warning a group sponsored by the Chinese state has been targeting US critical infrastructure and could direct their efforts to others worldwide. The Chinese group is called Volt Typhoon and has been targeting a range of infrastructure ranging from communications, to construction, to utilities, according to Microsoft, which uncovered the activity. The cybersecurity advisory has been issued by multiple bureaus including the US National Security Agency, New Zealand's National Cyber Security Centre as well as Australian, Canadian and UK cyber security agencies.

"The National Cyber Security Centre (NCSC) has joined international partners in publishing a technical advisory to highlight malicious cyber activity associated with a People's Republic of China (PRC) state-sponsored cyber actor," a statement from the agency said. "The activity has been observed affecting networks across United States critical infrastructure sectors and the techniques described could be used to impact other sectors." NCSC said the advisory is being published to provide New Zealand critical infrastructure operators and cyber defenders with information that will enable them to detect this activity.

World

FBI says it has sabotaged hacking tool created by elite Russian spies

The FBI has sabotaged a suite of malicious software used by elite Russian spies, according to U.S. authorities, providing a glimpse of the digital tug-of-war between two cyber superpowers. Senior law enforcement officials said FBI technical experts had identified and disabled malware wielded by Russia's FSB security service against an undisclosed number of American computers, a move they hoped would deal a death blow to one of Russia's leading cyber spying programs.

Australia's Medibank served with third class-action suit over cyber breach

Australia's Medibank Private Ltd said it was served with another class-action suit related to the cyber hack incident last year in which personal data of current and former customers was leaked on the dark web. The third class-action suit related to the incident was filed in the country's federal court by law firm Slater & Gordon on behalf of affected current and former Medibank customers, and healthcare service providers. Among the many breaches reported by Australian companies since late last year, Medibank had disclosed that a hacker stole personal information of 9.7 million current and former customers and released the data on the dark web. In a statement on its website, Slater & Gordon alleged that the health insurer failed to protect, or take reasonable steps to protect the personal information of its customers, thereby breaching consumer law and privacy principles. In recent months, similar class action suits against the company have been filed by law firms Baker & McKenzie and Quinn Emanuel Urquhart & Sullivan.

Cyber-attack to cost outsourcing firm Capita up to £20m

The outsourcing firm and government contractor Capita has revealed it will take a hit of up to £20m from a recent cyber-attack in which some customer, supplier and staff data was accessed by hackers. The group, which is a major contractor for local authorities, said investigations into the incident suggested that some data was accessed but that this was from less than 0.1% of its server estate. It said it had taken "extensive steps" to recover and secure the data contained within the affected server estate, and to "remediate any issues arising from the incident". It expects the bill for the cyber-attack to reach between £15m and £20m, covering specialist professional fees, recovery and remediation costs, as well as investment to reinforce its cybersecurity defences and strengthen its IT security.

More Sophisticated and Persistent Threats So Far In 2023

The pace of technological innovation has led to a transformation in many areas of our lives. In 2023, although it is only Spring, the impact of emerging technologies including artificial intelligence/machine learning, 5G, IoT, and quantum are significantly impacting everything connected to the internet. The introduction of these potentially disruptive technologies do have implications on cybersecurity and the challenges of keeping us safe. In particular, AI is the hot topic of focus as generative artificial intelligence can leverage ChatGPT-powered for code, and AI/machine learning to amplify social engineering capabilities and help identify target vulnerabilities for hackers. As data continues to be produced and stored in greater volumes, and as connectivity greatly expands globally on the internet, the attack surface has become more exploitable with gaps and vulnerabilities for criminal and nation state hackers and they are taking advantage.

North Korean hackers impersonated journalists to gather intel from academics and think tanks

Security researchers have warned that North Korean government-backed hackers are impersonating journalists to gather strategic intelligence to help guide the country's decision making. SentinelLabs researchers said that they had linked a social engineering campaign targeting experts in North Korean affairs to a North Korean advanced persistent threat (APT) group known as Kimsuky. The group, also known as APT43, Thallium and Black Banshee, has been operating since at least 2012 and is known for using social engineering and targeted phishing emails and to gather sensitive information on behalf of the North Korean regime. Kimsuky's latest social engineering campaign targeted subscribers of NK News, an American subscription-based website that provides stories and analysis about North Korea.

The cyber gulag: How Russia tracks, censors and controls its citizens

When Yekaterina Maksimova can't afford to be late, the journalist and activist avoids taking the Moscow subway, even though it's probably the most efficient route. That's because she's been detained five times in the past year, thanks to the system's pervasive security cameras with facial recognition. She says police would tell her the cameras "reacted" to her — although they often seemed not to understand why, and would let her go after a few hours. "It seems like I'm in some kind of a database," says Maksimova, who was previously arrested twice: in 2019 after taking part in a demonstration in Moscow and in 2020 over her environmental activism. For many Russians like her, it has become increasingly hard to evade the scrutiny of the authorities, with the government actively monitoring social media accounts and using surveillance cameras against activists.

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.

9/05/2023 – CISA and Partners Disclose Snake Malware Threat From Russian Cyber Actors

Our Views:

Cyber Insurance

What is cyber insurance?

Smart organisations manage cybersecurity within their overall risk management strategy. Cyber insurance may be considered as one of the tools available for use in risk management to help specifically mitigate technology risk. Cyber insurance (sometimes known as cyber-liability insurance) is a formal policy or contract between an insurer and an organisation intended to mitigate risk exposure by offsetting the potentially devastating costs related to computer or network-based incidents. Risk transference is a technique typically used for high impact but low likelihood risks, and with cyber insurance organisations hedge their cyber risk by paying a premium to transfer this risk to a third party (the insurer). Cyber insurance is designed to fill the gap that traditional insurance policies don't cover and is often triggered by attacks such as ransomware and business email compromise (BEC).

Cyber insurance, in various forms has been around since the 1990s, however in recent years the demand for this type of insurance has grown due to the increasing amount of financial loss experienced by organisations as a result of cyber-attacks. The global cyber insurance market is now estimated to be valued at $33.4 billion by 2027, according to Global Data.

Why would you consider purchasing cyber insurance?

As a result of widespread digital transformation, cybercrime has become a sophisticated and fast-growing threat. Recent well publicised data breaches in New Zealand and beyond have demonstrated how the loss of personal data may have far-reaching implications for an organisation, its customers, and its teams. The variety of incidents also shows how no industry is immune to these attacks.

The impact from the loss of personally identifiable information (PII), sensitive data, proprietary information and intellectual property is significant. When this data falls into the hands of a criminal or competitor it can severely disadvantage an organisation. Equally the large expenses associated with downtime or loss of revenue when handling a cyber incident can prove to be an existential threat to many organisations. A cyber-attack can financially harm your organisation in many ways, including:

- Lost income and productivity
- Regulatory fines or additional cost associated with compliance
- Brand and reputation damage
- Third party liability
- Crisis management expenses
- Legal defence expenses

Having cyber insurance will not stop an attack, but it will help a business recover and minimise any potentially catastrophic failures. As a result, many organisations are turning to cyber insurance as a means of protection against some of these negative impacts.

Who needs it?

Organisations of all sizes and across all industries collect, create, and hold information; and rely on technology to operate. Therefore, most organisations may benefit from cyber insurance. Assessing the unique cyber risk profile of your organisation is vital however for understanding how and how much cyber insurance may play a role in your overall risk management strategy. An organisation may be particularly exposed to cyber risk if it:

- Frequently handles large financial transactions.
- Relies on vendors, independent contractors, and service providers.
- Gathers and stores personal or sensitive information.
- Has a high degree of dependence on electronic processes.
- Has an online presence.
- Enables remote working.
- Must comply with New Zealand or international privacy legislation.
- Must comply with Payment Card Industry Security Standards or other specific industry-based requirements.

Continue reading our views on cyber insurance and more in our premium edition of the bulletin.

Click here to join.

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: