NZ Incident Response Bulletin

Standard Edition – March 2023 – Issue #50

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

Injunctions – A Valuable Tool in Data Breach Toolkit

Protecting people in the middle of a fast-moving data breach must always be prioritised. Privacy Commissioner Michael Webster says the February injunction issued by the High Court to stop people sharing and using the data that was stolen in last year's breach of service provider Mercury IT is great evidence of that. "It proves the value of accessing the courts quickly to protect the public's interests."

The High Court of New Zealand has made permanent an injunction that prevents anyone from storing, publishing, sharing, or accessing files obtained from the attack on Mercury IT systems. Mr Webster says injunctions are another tool that agencies can use to protect information compromised in a cyber-attack or other form of privacy breach. "You have to act fast. It might sound drastic but reaching out to the courts can help prevent further harm by making it clear to everyone, that no one should breach the confidences that apply to that compromised data. The injunction applies to everyone from individuals to the news media and bloggers."

Digital infrastructure to drive 49% of business revenue

Digital infrastructure is set to drive 49% of business revenue in Australia and New Zealand (ANZ) by 2027, according to Lenovo. Lenovo, along with AMD, launched a new InfoBrief titled 'CIO Technology Playbook 2023' that aims to highlight the opportunities, challenges, and considerations for CIOs in today's data-driven economy to help them make the right IT investments. With the rapid digital transformation in the Asia Pacific, organisations are expected to generate as much as 43% of the revenue from digitally connected products, services, and customer experiences by 2027.

The results observed show concerns among CIOs around macroeconomic factors affecting business growth in 2023 and early 2024. Respondents in ANZ cited 'high inflation' (55%) as the topmost concern in 2023, followed by 'human capital shortage' (47%) and 'high energy prices' (46%) as the other key challenge areas. "In the current economic climate, ANZ businesses are striving to optimise their resources. CIOs are prioritising cyber security to combat rising cyber threats. Meanwhile, the focus on digital transformation through AI/ML and edge computing is vital to cut costs and meet the demand for using these technologies in security, fraud/risk management, and IT operations," says Manu Mehra, Managing Director - Australia and New Zealand, Lenovo ISG.

Scammers taking advantage of Cyclone Gabrielle tragedy

Scammers are taking advantage of the tragedy from Cyclone Gabrielle to try and make money, authorities are warning. At least one bank has received several reports of scammers targeting its customers. Westpac's head of financial crime Mark Coxhead said it had heard of about a dozen reports of attempted scams but said he feared that number could rise. "It's really common, and it's really sad, but scammers are trying to take advantage of people when they're at their lowest, they're trying to catch you off guard," he said.

Data ethics group discusses constraints of not having regulatory authority

A data ethics group has raised issues about whether it needs more teeth to act as a government watchdog. The board, which advises on issues such as algorithms, data collection, and ethics, restarted in October after not meeting since 2020.

A report into the data ethics advisory group (DEAG) in 2020 found its role was confined by looking into issues that ministries and agencies referred to it. Official Information Act documents show its chair, who resigned two years ago, said it needed a structural fix and to report directly to ministers.

World

Australia setting up new agency to fight cyber-criminals

A new federal agency is being set up to protect Australians from mass cyber-attacks. The Federal Government wants to minimise the risk of future mass cyber-attacks like those against Optus and Medibank last year. To do so, it is overhauling the previous government's cyber security strategy, which involves appointing a cyber security coordinator to lead the charge on things like responding to online threats and attacks. This comes as the government meets business leaders to discuss how-to step-up defences in corporate and public systems. The aim is to keep Australian data and services safe as cyber threats evolve.

Prime Minister's Cyber Security Roundtable

Australian Prime Minister, the Hon Anthony Albanese MP, has led a Cyber Security Roundtable, focused on the whole-of-nation effort required to protect Australians and our economy, with the aim of making Australia the most cyber-secure nation by 2030. Attending the roundtable were leaders from the public service and intelligence agencies, and independent experts from business, industry and civil society. Ideas discussed included incentivising best practice cyber behaviours, growing Australia's cyber security sector and raising national cyber awareness, to shape a new strategy. The federal government also announced it will establish a Coordinator for Cyber Security, supported by a National Office for Cyber Security within the Department of Home Affairs, to ensure what the government says is a centrally coordinated approach to deliver the government's cyber security responsibilities.

Top US cyber official warns software firms aren't doing enough to stop damage from hackers from China and elsewhere

Chinese hackers are too frequently going "unidentified and undeterred," and software companies aren't doing enough to secure their products from cyber-attacks that "can do real damage" to US interests through the loss of trade secrets, a top US cyber official said. "The risk introduced to all of us by unsafe technology is frankly much more dangerous and pervasive than the spy balloon, but somehow we've allowed ourselves to accept it," US Cybersecurity and Infrastructure Security Agency Director Jen Easterly said in a speech at Carnegie Mellon University. Easterly was referring to a suspected Chinese surveillance balloon that flew over multiple US states before the US military shot it down on February 4. The episode has increased tensions in US-China relations and caused US Secretary of State Antony Blinken to postpone a trip to Beijing.

Seven Russians sanctioned over ransomware cyber-crime

Seven Russian men have been sanctioned by the UK and US for having links to recent ransomware attacks. The UK's Foreign Office, along with US authorities, has released pictures of the men, frozen their assets and imposed travel restrictions. US authorities have accused them of being members of loosely defined Russian-based hacking network Trickbot. Ransomware strains Conti and Ryuk extorted at least £27m in ransoms from 149 British victims. "This is a hugely significant moment for the UK and our collaborative efforts with the US to disrupt international cyber-criminals," said National Crime Agency director general Graeme Biggar. "The sanctions are the first of their kind for the UK and signal the continuing campaign targeting those responsible for some of the most sophisticated and damaging ransomware that has impacted the UK and our allies," he said.

Tonga is the latest Pacific Island nation hit with ransomware

Tonga's state-owned telecommunications company has been hit with ransomware, it warned customers on Monday. Tonga Communications Corporation (TCC) — one of two telecoms companies in the country — published a notice on Facebook saying the attack may slow down administrative operations. "Ransomware attack has been confirmed to encrypt and lock access to part of TCC's system. This does not affect voice and internet service delivery to the customers, however, it may slow down the process of connecting new customers, delivering of bills and managing customers' enquiries," the company said.

Cyberattacks hit data centers to steal information from global companies

Cyberattacks targeting multiple data centers in several regions globally have been observed over the past year and a half, resulting in exfiltration of information pertaining to some of the world's biggest companies and the publishing of access credentials on the dark web, according to cybersecurity company Resecurity. Most recently, credentials related to data center organizations and acquired during various episodes of the malicious campaign were published in the underground forum Breached.to and detected by researchers Monday. Some fragments of that particular data cache have also been shared by various threat actors on Telegram.

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.

23/02/2023 - CISA Urges Increased Vigilance One Year After Russia's Invasion of Ukraine

Our Views:

Making Cyber Security Awareness Training Engaging

Phishing and credential harvesting remain the most reported incident category in recent years, responsible for the greatest number of business compromises. Therefore, the necessity to invest in cybersecurity training and awareness initiatives has become paramount. Regular cyber training can positively influence your business cyber culture and empower your team to protect themselves and your business from social engineering attacks however, many people find cyber security dry, unapproachable and boring…gasp – yes, it's true – even sci-fi fans are unlikely to look forward to more compulsory risk training modules added to an already full day. So, how can businesses design programmes that are engaging and encourage full participation?

Use Real-World Examples

Learning from a textbook is boring. People engage with stories. Since the origins of humanity, sharing stories (sometimes over food or fire) has allowed humans to learn. Sharing successes and failures are equally important. Telling real-world tales of how incidents have happened or nearly happened, mistakes that were made or avoided, and reflecting on how things could have gone differently allows us to engage and visualise an incident happening to us.

Use Multi-disciplinary Trainers

Teams need to find a trainer relatable to fully engage with the content. Using team members from various backgrounds can be key to ensuring messages are contextualised and understood. As cyber security is everyone's responsibility, try using team members from multiple different areas to lead cyber training (e.g. Marketing, Human Resources, Customer Care). Each group will describe cyber and its impacts and importance in a different manner and these teams often hold great communicators.

Mix up the Medium

Rather than relying on one method to get your message across, ensure your programme involves various ways to increase awareness. For example, if you run an online phishing quiz or training video in the first quarter, then try a face-to-face presentation, Q&A or cyber simulation in the second. Posters, wallets or desk cards could be introduced in the third quarter, and a quiz run in the last.

Walk The Talk

Culture is driven from the top. Leaders need to be advocates for the training and awareness and demonstrate support by participating and caring about its ongoing success.

Make it Fun!

Make sure any messages are delivered with fun and humour! Try using rewards for both participation and as prizes.

Use your Vendors

Invite a variety of vendors that have credible content and experience to share. Just ensure the focus is not sales and remains system agnostic. Many vendors will be happy to contribute experience and stories from a wide range of industries as when security is lifted in one link in the supply chain, it makes everyone more secure.

Keep it Short (but Regular)

Keep it brief. Holding the attention of busy teams requires targeted and efficient delivery. Additionally, studies have shown that people start to forget the lessons from phishing training after about six months indicating regular refreshers are vital. Shorter but regular cyber training is recommended.

Games for the Tech Savvy

There are plenty of online games for more tech-savvy or cybersecurity focussed individuals to engage in and play to both test their skills and enhance learning. Some to try include:

- Cyber Challenge - Developed by the US Department of Defence, Cyber Challenge involves solving cyber threats and looking at roles in cyber.
- Cybersecurity Lab - A browser-based game involving cracking passwords, creating code and defeating malicious adversaries.
- Keep Tradition Secure - Involves answering a series of cybersecurity questions to track down a hacker on a college campus.
- picoCTF - Developed by Carnegie Mellon and similar to capture the flag challenges.

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: