NZ Incident Response Bulletin

Premium Edition – April 2023 – Issue #51

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

White House official says door is open for further talks with New Zealand

A top-ranking White House official says New Zealand has been receptive to working with AUKUS in the cyber arena. Kurt Campbell, Joe Biden's National Security Council co-ordinator for the Indo Pacific, briefed media in Wellington this morning on the defence pact between Australia, the UK and the US. He said the US was now looking for other working group partners, and from his perspective the door was open for further talks with New Zealand.

"We agreed that we would launch the critical components of AUKUS, and then take steps to look at other partners," he said. "I will say, we've been gratified by how many countries want to join with us to work with cutting-edge technologies like in the cyber arena, hypersonics, you can go down a long list and it's great to hear that New Zealand is interested." Campbell confirmed the United States was continuing its diplomatic push in the Pacific.

Nearly 15,000 NZ driver licences exposed in Aussie hack

1News can confirm that nearly 15,000 New Zealand driver licences have been caught up in the Latitude Financial breach so far, with the NZTA bracing for many more to be affected. In a statement, Waka Kotahi said it "can confirm that 14,925 New Zealand driver licence cards were impacted by the first breach identified by Latitude Financial Services".

Waka Kotahi says it's still working to assess the scope of the exposure. "They will be communicating next steps directly to their impacted customers." Today, in a stark revision to its initial estimates, Latitude Financial, the company said the number of Australian and New Zealand driver licence numbers stolen had blown out to approximately 7.9 million "of which approximately 3.2 million, or 40%, were provided to us in the last 10 years." In addition, Latitude Financial has said 53,000 passport numbers were taken too.

Research Shows New Zealanders Have Fears About Privacy

Privacy breaches are costing millions of dollars worldwide with agencies and businesses near and far in the crosshairs of internet criminals. This week an Internet NZ report revealed New Zealanders want their privacy kept safe and respected. Privacy Commissioner Michael Webster says privacy is a basic right people should be able to expect. However, it was important that members of the public beef up their own education too about how to keep their lives private because prevention is always better than cure. The report found three quarters of New Zealanders are worried about children accessing inappropriate material online. The other top concerns were online crime, security of personal data, cyber bullying, and threats to privacy.

Consistent with last year's report, in the past 12 months two thirds of New Zealanders have chosen not to use at least one online service because of security or privacy concerns. "The internet holds a lot of promise for people and allows them to connect with their communities and the rest of the planet. It's important people can connect and trust, so it will be incredibly upsetting if we lose that because agencies don't value the crucial importance of privacy."

Report On Police Management of Fraud

In a report released in November 2022, the Independent Police Conduct Authority found major deficiencies in the way in which Police respond to fraud complaints. It recommends the development of a fraud prevention strategy incorporating both public and private sector agencies led by Police. The 45 page report provides a comprehensive assessment of fraud and police fraud management within New Zealand. According to the report:

More New Zealanders are victims of fraud and deception offences than of any other crime, yet the complaints outlined in this report, combined with very low rates of recording, charging and prosecution of these offences, show that in relation to fraud there are significant opportunities for Police to lead across the public and private sectors to achieve their stated mission "to prevent crime and harm through exceptional policing".

World

Ransomware Attacks Have Entered a 'Heinous' New Phase

In February, attackers from the Russia-based BlackCat ransomware group hit a physician practice in Lackawanna County, Pennsylvania, that's part of the Lehigh Valley Health Network (LVHN). At the time, LVHN said that the attack "involved" a patient photo system related to radiation oncology treatment. The health care group said that BlackCat had issued a ransom demand, "but LVHN refused to pay this criminal enterprise." After a couple of weeks, BlackCat threatened to publish data stolen from the system. "Our blog is followed by a lot of world media, the case will be widely publicized and will cause significant damage to your business," BlackCat wrote on their dark-web extortion site. "Your time is running out. We are ready to unleash our full power on you!" The attackers then released three screenshots of cancer patients receiving radiation treatment and seven documents that included patient information.

IPH Confirms Cyber Attack

Australian listed intellectual property services firm IPH has confirmed that it has been subject to a cyber-attack. The company asked the Australian Securities Exchange for a trading halt while it investigated a possible breach. In an ASX statement the company said on March 13 it detected "unauthorised access to a portion of its IT environment." "Based on preliminary analysis, it appears the incident is primarily limited to the document management systems of the IPH head office, and two IPH member firms," it said. The statement said their practice management systems were also breached. Information that may have been breached includes business admin documents, client documents and correspondence, and IP case management information.

Australia demands Russia crack down on cyber criminals

One of Australia's top government bureaucrats on Wednesday demanded Russia crack down on the large number of cyber criminals operating in the country, saying their actions posed a threat to national security. The comments come as Canberra reforms its cybersecurity policy following a raft of cyber-attacks on some of the country's largest companies. "The greatest density of cyber criminals, particularly those with ransomware, are in Russia," Michael Pezzullo, Secretary of the Department of Home Affairs, told the AFR Business Summit in Sydney. "They are not a rule of law country and the thought that you can apply conventional law enforcement disciplines ... is completely naive. We call on the Russian government to bring those hackers to heel." A spokesperson for the Russian embassy did not immediately respond to a request for comment. The Australian government last month said it planned to overhaul its cybersecurity rules as well as set up an agency in Pezzullo's department to coordinate government investment in the field and help coordinate responses to hacker attacks.

AT&T Informs Nine Million Customers about Data Breach

AT&T is informing customers about a data breach at a vendor's system that allowed threat actors to gain access to AT&T's Customer Proprietary Network Information (CPNI). The incident came to light after customers posted the email communication from AT&T on community forums to know if it was legitimate or email fraud. "We recently determined that an unauthorized person breached a vendor's system and gained access to your 'Customer Proprietary Network Information' (CPNI)," AT&T said in the email. Approximately nine million customers' CPNI was accessed by the threat actors. CPNI is the information that telecommunication companies in the US acquire about subscribers and includes information on the services they use, the amount paid for the services, and the type of usage.

UK Crypto Firm Loses $200m in Cyber-Attack

UK crypto startup Euler Labs has suffered a devastating cyber-attack, in which threat actors managed to steal close to $200m from its DeFi lending protocol. The firm provides a DeFi protocol on Ethereum that it claims allows users to lend and borrow almost any crypto asset. However, yesterday hackers managed to exploit a vulnerability in its code which enabled them to steal around $199m in various digital currencies: USDC ($34.1m), Dai ($8.8m), Wrapped Bitcoin ($18.9m) and Staked Ether ($137.1m), according to blockchain analysis firm Elliptic. "Flash loan attacks involve taking out large, short-term uncollateralized crypto loans from a DeFi service, and using the large sums involved to manipulate the market and other DeFi services in their favor," the firm explained. "The proceeds of the attack are already being laundered through Tornado Cash, a decentralized mixer that has been sanctioned by the US government."

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.

21/03/2023 – CISA and NSA Release Enduring Security Framework Guidance on Identity and Access Management

16/03/2023 – StopRansomware: LockBit 3.0

Our Views:

Investigating Fraud in New Zealand

"Fraud" is an activity where the perpetrator deceives the victim in order to obtain a benefit. According to the Association of Certified Fraud Examiners (ACFE) and Black's Law Dictionary, fraud becomes a crime when it is a "knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment". In other words, if you lie in order to deprive a person or organisation of their money or property, you're committing fraud.

Due to the increasing prevalence of technology in every aspect of our lives, a significant amount of fraud is now committed using the internet, and New Zealand Police figures report that up to 97% of "cyber-enabled" crimes are fraud. Examples of fraud include fraudulent online trading, online agency fraud, relationship scams, identity theft, credit card/EFTPOS fraud, amongst others.

Fraud is a significant issue in New Zealand, with 8% of all New Zealand adults being a victim of fraud or deception in 2021. This is higher than any other offence type reported. Unfortunately, fraud is also significantly underreported compared to all other offences, so this 8% is likely to be the tip of the iceberg. Therefore, while the scale of the known issue is concerning, the possible scale of the full problem is even worse. The Police Financial Crimes Unit has estimated that between 20 and 30 million dollars per year are lost by New Zealanders alone because of scams.

Fraud is a criminal offence in New Zealand, with the Crimes Act 1961 outlining the offences that relate to deception, dishonesty, forgery and crimes involving computers. However, despite criminal legislation existing to combat fraud, there are current concerns that this issue is not being investigated or prosecuted effectively in New Zealand, and victims are not well supported. As a result of receiving 52 complaints between 2018-2020 from the public about the police in response to fraud, in 2022 the Independent Police Conduct Authority (IPCA) conducted a review of the police management of fraud allegations and concluded there are systemic issues preventing an effective response.

One of the numerous example complaints investigated in the review involves a situation whereby two company directors reported to the police that the third co-director had defrauded the company of around $150,000. The police initially advised the complainants to try to negotiate with the offender and get the money back. When unsuccessful the complainants sought a formal prosecution. They were again advised by the police that they needed to gain the evidence themselves. Two years later, the investigation had not made any progress, and the police once again informed the complainants to gather further evidence themselves. Uncomfortable with making the enquiries required to gain this evidence, the complainants were informed the case would be closed. Once a complaint was laid, the police reopened the case however despite this crime being first reported in 2017; it was only in June 2022 that the complainant's statements were completed.

Issues that prevent effective investigation of these crimes raised in the IPCA's reviews report include:

A pervasive and incorrect perception that fraud is of low importance and has little impact

The impact of fraud can be existential on businesses, and the perception that these crimes are not important within both the Police and society in general must change, or we will face increasing amounts of loss driven by the complacency of investigation and continued criminal success in this area.

Variable processes for receiving, categorising, and prioritising fraud investigations

Variable processes exist to report fraud which leads to inconsistency and an unknown amount of fraud offences never being captured by the system. Fraud offences that are reported along with computer crime are automatically categorised as category four cases meaning they receive the lowest priority for investigation. Finally, once categorised, the cases undergo an initial file assessment derived from a series of weighted factors that indicate the solvability of the crime. This process results in a "solvability" score being assigned to the case. If the score is under 7 then early case closure or no investigation is recommended. Unfortunately, the weighted factors to derive this score do not reflect the nature of electronic fraud today. Electronic crime means it is rare for a victim to be able to identify or provide a description of the offender lowering the score assigned. Additionally, the use of a vehicle lifts the score, which is highly unlikely in any online fraud attempt. Factors that could be used to provide evidence in an investigation of electronic fraud are not included in the scoring system, such as the presence of a digital footprint used by an offender. This process results in fraud being handled and categorised as low priority regardless of whether it involves substantial amounts of money or has significant victim impact.

Inconsistent and inadequate investigation structures

There is no national Police coordinator for fraud leading to a lack of investigative information sharing and consistency across New Zealand regions.

Lack of a victim focus

As fraud is often miscategorised as unimportant or low priority the victims of fraud are currently not receiving adequate attention and support. Fraud victims report serious stress-related illness, and underestimating the impact of this crime is hurting society.

Inadequate expertise and training

The IPCC report highlights the lack of specialist fraud training that the New Zealand Police receive. Often these cases require specialist forensic accounting or digital forensic expertise, which is currently also not always available and puts the investigation of these crimes in the "too hard" basket too frequently.

Despite an increasing number of fraud cases being reported to the police between 2016 and 2020, the proportion of these leading to charges significantly decreased. Fundamentally the way we think about fraud and the way we investigate fraud must change to keep up with the avalanche of this type of crime. This problem is not unique to New Zealand, with the Police Foundation in England and Wales stating that "40% of all crime is now fraud, most of which is cyber-enabled. Yet we are tackling crime and disorder of the digital age with an analogue policing approach".

Recommendations

It is our view that until the findings from the IPCC report are accepted and its recommendations implemented it is unlikely that you will receive an adequate level of advice, follow-up, or action from the appropriate authorities alone when your business suffers fraud. We, therefore, recommend that if you suspect fraud, you consider engaging additional assistance to investigate, procure evidence, and provide expertise and advice on steps you can take in addition to reporting this crime through police channels.

There are a range of fraud prevention strategies you can apply to reduce the risk of falling victim. Several examples include:

- Keep abreast of Fraud Risk Management, the New Zealand Government provides a helpful list of resources here.
- If not already, implement a set of Cyber Security Controls. One such example is the CIS Controls.
- Implement a third party whistleblowing platform to encourage people to report instances of fraud.
- Consider having an incident response and forensic technology provider on retainer.

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: