NZ Incident Response Bulletin

Standard Edition – December 2022 – Issue #47

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

As reported in the media, a number of New Zealand organisations have been impacted by a cyber-attack. Newsworthy articles will be referred to in next month's Bulletin.

Australia wants NZ support on cyber-attacks, foreign interference

Foreign interference is threatening decades of work on building social cohesion in Australia and New Zealand, an Australian minister has said in a speech also promising progress on the rights of Kiwis across the ditch

The Australian government wants to work with New Zealand on foreign interference and taking down hackers after a spate of devastating cyber-attacks in the country, a senior minister says.

Australian home affairs minister Clare O'Neil, who holds responsibility for cyber security and immigration among other issues, has also provided further reassurances regarding the rights of Kiwis living in Australia - although without any specific details on new progress.

Military exercise: Defence force test cyber skills

Eleven New Zealand Defence Force personnel have taken part in a United States exercise designed to build a community of military defensive cyber operators armed with skills to defend against modern digital threats. This year's NZDF contribution to Exercise Cyber Flag in Suffolk, Virginia included personnel drawn from the NZ Army Land Component and Special Operations Component. Amongst these were Regular Force soldiers as well as part-time Army Reserve Force soldiers and a civilian from the NZDF's Defence Cyber Security Centre. The exercise, hosted by US Cyber Command late last month, was conducted alongside military partner nations.

Archives NZ reinstates online search tool after data mishap

Archives NZ is making its online search tool available to all users again, after a shutdown caused by restricted record titles mistakenly being made public. It has been investigating what it said was "a potential security and privacy" breach for over a week. Archives said this afternoon it was satisfied there has been no privacy breach from the records.

1.8m Kiwi phone numbers potentially exposed during major WhatsApp data scrape

More than 1.8 million New Zealand WhatsApp users could be at risk after an alleged major data scrape potentially exposed their phone numbers. Earlier this month a user on a hacking forum claimed to be selling a vast amount of records of users of the app, which had been gathered throughout November. 1News reported the unnamed user, who claimed to have scraped the phone numbers of 1,824,589 New Zealand WhatsApp accounts.

Education report recommends more cybersecurity investment as risk grows

An assessment has found big gaps in schools' cybersecurity and recommends a multi-million-dollar boost to school funding for IT. The report, provided to RNZ under the Official Information Act, recommended setting minimum standards and providing more central support for schools. The assessment was prompted by growing concern about schools' vulnerability to hackers and was completed in March. It said the Education Ministry was developing a business case for a multi-year work programme to address longer-term problems.

World

Cyberattack Causes Trains to stop in Denmark

According to Danish broadcaster DR, all trains operated by DSB, the largest train operating company in the country, came to a standstill on Saturday morning and could not resume their journey for several hours. While this may sound like the work of a sophisticated threat actor targeting operational technology (OT) systems in an effort to cause disruption, it was actually the result of a security incident at Supeo, a Danish company that provides enterprise asset management solutions to railway companies, transportation infrastructure operators and public passenger authorities.

Medibank Refuses to Pay Ransom After 9.7 Million Customers Exposed in Ransomware Hack

Australian health insurer Medibank today confirmed that personal data belonging to around 9.7 million of its current and former customers had been accessed following a ransomware incident. The attack, according to the company, was detected in its IT network on October 12 in a manner that it said was "consistent with the precursors to a ransomware event," prompting it to isolate its systems, but not before the attackers exfiltrated the data.

Australia sees spike in cyber attacks from criminals and states

Cyber-attacks against Australia from criminals and state-sponsored groups jumped last financial year, with a government report released on Friday equating the assault to one attack every seven minutes. The Australian Cyber Security Centre (ACSC) received 76,000 cybercrime reports last financial year, up 13 percent from the previous period, according to its latest annual cyber threat report. While just over half of attacks targeted individuals for fraud and theft, the report warned that state-sponsored attackers made cyberspace a "battleground" and cited attacks from China's Ministry of State Security, Iran and Russian state-linked groups.

Russian-Canadian National Charged Over Involvement in LockBit Ransomware Attacks

The U.S. Department of Justice (DoJ) has announced charges against a dual Russian and Canadian national for his alleged participation in LockBit ransomware attacks across the world. The 33-year-old Ontario resident, Mikhail Vasiliev, has been taken into custody and is awaiting extradition to the U.S., where he is likely to be sentenced for a maximum of five years in prison. Vasiliev has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands, according to a criminal complaint filed in the District of New Jersey.

Whoosh confirms data breach after hackers sell 7.2M user records

The Russian scooter-sharing service Whoosh has confirmed a data breach after hackers started to sell a database containing the details of 7.2 million customers on a hacking forum. Whoosh is Russia's leading urban mobility service platform, operating in 40 cities with over 75,000 scooters. On Friday, a threat actor began selling the stolen data on a hacking forum, which allegedly contains promotion codes that can be used to access the service for free, as well as partial user identification and payment card data.

Advocates had warned of the dangers of a real estate data breach. It just happened

Australian real estate agency Harcourts has revealed it was affected by a cyber attack last month, with the personal information of tenants, landlords, and tradespeople potentially exposed. In an email sent to customers of the Melbourne City franchisee of Harcourts, the company said it became aware on 24 October that an "unknown third party" had accessed its rental property database.

Daixin Ransomware Gang Steals 5 Million AirAsia Passengers' and Employees' Data

The cybercrime group called Daixin Team has leaked sample data belonging to AirAsia, a Malaysian low-cost airline, on its data leak portal. The development comes a little over a week after the company fell victim to a ransomware attack on November 11 and 12, per DataBreaches.net. The threat actors allegedly claim to have obtained the personal data associated with five million unique passengers and all of its employees. The samples uploaded to the leak site reveal passenger information and the booking IDs as well as personal data related to the company's staff.

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.

10/11/2022 - CISA Releases SSVC Methodology to Prioritize Vulnerabilities

1/11/2022 - OpenSSL Releases Security Update

Our Views:

Cloud Based Document Review Tools

As the number and severity of data and privacy breaches occur do you mean increase, the forensic process of collecting evidence for legal review can be a complicated and expensive process, carrying risks of missing key data. These are the same challenges faced by experts and lawyers working on matters such as fraud, misconduct and other employment investigations.

As defined by the Electronic Discovery Reference Model (EDRM):

Document review is a critical component to most litigation and is used to identify responsive documents to produce and privileged documents to withhold. It is the time where the legal team can begin to gain a greater understanding of the factual issues in a case and where legal strategies can emerge and begin to develop based on the type of information that is found in the collection of documents. There will inevitably be different strategies implemented for reviewing documents in preparation for production versus documents produced by opposing counsel, however the common thread is the need (a) to understand the scope of the review, (b) to put in place supervision and procedures for managing the reviewers and (c) to select the appropriate vendor, tools and platform for the review.

Out of necessity, a new industry has emerged where software vendors offer their solutions to various challenges such as the size of the dataset, the complexity of the file types, and ease of review. In the first instance, affected data sets are typically processed using an 'Early Case Assessment' tool, which triages and prioritises documents that are likely to cause serious harm as defined in the New Zealand Privacy Act 2020. These documents are then transferred to a review suite that will allow lawyers and other subject matter experts review the data.

Over recent years, there has been a considerable shift from software vendors to offer a cloud-based review solution. Faced with an urgent matter such a privacy breach, it can be difficult to quickly choose an option to suit your requirements.

Given your review requirements may increase over the course of the matter, we recommend selecting a comprehensive document review platform that has the flexibility and scale to manage any matter regardless of size and scope. With recent advances in technology, you should take advantage of the options available to accelerate and prioritise your review. Along with the basic features of search, filtering, and document organisation, advanced features including 'active learning' and 'artificial intelligence' may also prove invaluable.

Several years ago, in preparation for the new breach notification requirements under the Privacy Act 2020, Incident Response Solutions developed a suite search parameter that aids in the efficient and accurate identification of at-risk documents. With recent advances in technology, we have recently completed a further round of tailoring to suit New Zealand legislation, including all 'Evidence of Identity' documents as defined by the Department of Internal Affairs.

By applying our tailored search parameters to the artificial intelligence engine, we can continuously evolve and improve upon the review experience by leveraging human coding decisions throughout the review. Each decision made by the subject matter expert is automatically incorporated into the training process to improve the effectiveness of the model and then present the most relevant documents to the user.

One of the key challenges we see when faced with such reviews, is the often-significant number of non-searchable documents. This is particularly prevalent in organisations that are required to conduct 'Know Your Customer' checks in accordance with the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. We have worked on numerous privacy breach reviews at law firms, where staff have scanned passports and driver licences and stored these in cloud-based email accounts. If such accounts are breached as a result of a successful phishing attack, the attackers can access and download these documents. As most of the documents are 'scanned', we firstly need to convert them to be text searchable by running an Optical Character Recognition (OCR) process. While the quality of the outputs from such OCR process will vary depending on the source document, it will increase your chances of locating key documents.

There are significant risks that result from a privacy breach or the need to investigate a fraud or employment matter. As forensic and incident response experts we know how important it is for the legal and review teams to have access to leading review solutions. We recommend selecting a review suite that offers a flexible 'anywhere anytime' solution. Further, the solution should also comply with security requirements, including mandatory two factor authentication to protect your client's data.

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: