NZ Incident Response Bulletin

Premium Edition – December 2023 – Issue #59

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.

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.

Not subscribed to our Premium Bulletin? Click here to join.

New Zealand

Money-motivated cyber attacks outnumber those carried out by nation-states – watchdog

Major financially motivated cyber-attacks in New Zealand have exceeded those launched by nation-states for the first time, and Artificial Intelligence (AI) looms as an ever-greater weapon, a new report says. In its latest annual threat report, the National Cyber Security Centre said the potential impact was growing - though the number of major attacks dropped slightly, to 316.

It had "observed rapid advances in AI and early signs of it being used in malicious cyber activity overseas. AI can quickly synthesise derivative malware that could evade technical detection capabilities. Big data could also enable the reconnaissance function of a malicious cyber campaign, including surmising connections between disparate pieces of personal or network information, or painting a picture of a victim's preferences, to inform the malicious cyber actor's approach."

The centre estimated it had deflected $65 million of harm to nationally significant organisations - such as those that run power, waste or water systems. "We see heightened determination from cyber-criminal actors attempting to extort payment from organisations."

National security threat – NZ's isolation no longer a guarantee of safety

The last time tensions in the world were this high was during the Cold War and New Zealand can no longer rely on its geographic isolation for security. US-China tensions, Russian threats, extremism and the danger of cyber warfare are all simmering in the background while politicians also contend with complex local problems. Speaking to The Front Page podcast off the back of co-editing a new book called State of Threat: The challenges to Aotearoa New Zealand's national security, Professor William Hoverd – the director at Massey University's Centre for Defence and Security – says the country now faces new internal and external threats.

Australia

Australia is simulating cyberattacks to prepare for the real thing

The release of the Albanese government's new cybersecurity strategy includes a significant expansion of simulated exercises to prepare hospitals, supermarkets, data storage providers and other businesses to deal with major hacks. The release of the plan follows on from the hacks on Optus and Medibank last year, the recent Optus outage and the attack on port operator DP World.

DP World Australia confirms employee data was stolen during cyber-attack, warns of further freight delays ahead of XMAS rush

The boss of Australia's largest ports operator has confirmed data from current and former DP World employees was stolen during a cyber-attack that shut down its operations around the country. DP World Australia stopped its operations at its ports in Melbourne, Sydney, Brisbane and Fremantle on November 10 in response to a cyber-attack, resulting in significant delays of goods coming in and out of the country. The company is responsible for 40 per cent of Australia's maritime freight, and the outage resulted in a backlog of 30,137 shipping containers stacked up at its depots around the country.

OAIC commences Federal Court proceedings against Australian Clinical Labs Limited

The Office of the Australian Information Commissioner (OAIC) has commenced civil penalty proceedings in the Federal Court against Australian Clinical Labs Limited (ACL) resulting from an investigation of its privacy practices. The investigation arose as a result of a February 2022 data breach of ACL's Medlab Pathology business that was notified to the OAIC on 10 July 2022. The OAIC Commissioner alleges that from May 2021 to September 2022, ACL seriously interfered with the privacy of millions of Australians by failing to take reasonable steps to protect their personal information from unauthorised access or disclosure in breach of the Privacy Act 1988. The Commissioner alleges that these failures left ACL vulnerable to cyberattack.

Telcos required to report on cybersecurity measures in bid to prevent repeat of 2022 Optus hack

Australia's telecommunications companies will be hit with new rules forcing them to update the federal government on their cybersecurity regimes. Last year's massive Optus cyber-attack forced the issue into the public spotlight, fuelling serious concerns about the preparedness of Australia's telecommunications sector to deal with hacks – in terms of protecting their services, and the sensitive customer data they hold.

Optus loses court bid to keep report into cause of 2022 cyber-attack secret

Optus has lost a bid in the federal court to keep secret a report on the cause of the 2022 cyber-attack which resulted in the personal information of about 10 million customers being exposed after a judge rejected the telco's legal privilege claim. After the hack, the company announced in October 2022 that it had recruited consultancy firm Deloitte to conduct a forensic assessment of what had led to the cyber-attack. Since then, the company has also faced an investigation by the Office of the Australian Information Commissioner (OAIC), and a class action case in the federal court. As part of the class action case, law firm Slater and Gordon, acting for the applicants, had sought access to the Deloitte report that was never made public. Optus had argued in court that the dominant purpose of the report was to assess the legal risk to the company. It claimed Deloitte's report would assist the company's internal and external lawyers on how to advise the company about the risks associated with the hack.

World

British Library suffering major technology outage after cyber-attack

The British Library suffered a technology outage after it was hit by a cyber-attack, affecting services online and its sites in London and Yorkshire. The British Library said it had launched an investigation into the incident with the support of the National Cyber Security Centre (NCSC) and other cybersecurity specialists.

Ransomware attack on China's biggest bank may have hit US Treasury market

A US unit of the Industrial and Commercial Bank of China (ICBC) was hit by a ransomware attack that disrupted some of its systems, reportedly hitting liquidity in US Treasuries which may have contributed to a brief market sell-off. ICBC Financial Services, which is headquartered in New York, said in a statement that the attack had been reported to law enforcement.

Law firm Allen & Overy hit by 'data incident'

Allen & Overy advised they had suffered a "data incident" after social media posts suggested it had been hacked by the Lockbit cybercrime gang. The attack comes after seven countries, including the United States and Britain, in June named Lockbit as the world's top ransomware threat. An Allen & Overy spokesperson said the firm had "experienced a data incident impacting a small number of storage servers", but its email and document management system had not been affected.

Ransomware gang files SEC complaint over victim's undisclosed breach

The ALPHV/BlackCat ransomware operation has taken extortion to a new level by filing a U.S. Securities and Exchange Commission complaint against one of their alleged victims for not complying with the four-day rule to disclose a cyberattack. The threat actor listed the software company MeridianLink on their data leak with a threat that they would leak allegedly stolen data unless a ransom is paid in 24 hours.

International Counter Ransomware Initiative 2023 Joint Statement

The 50 members of the International Counter Ransomware Initiative (CRI) met for the third convening. Members reaffirmed their joint commitment to building the collective resilience to ransomware, cooperating to undercut the viability of ransomware and pursue the actors responsible, countering finance that underpins ransomware, working with the private sector to defend against ransomware attacks, and continuing to cooperate internationally across all elements of the ransomware threat.

Canadian former intelligence chief found guilty of leaking state secrets

A jury has found the former head of the Royal Canadian Mounted Police intelligence unit guilty of leaking state secrets, the first time a Canadian has been convicted under the country's Security of Information Act. Jurors said Cameron Ortis was guilty of three counts of violating the act and one count of attempting to do so. They also found him guilty of breach of trust and fraudulent use of a computer. The charges followed one of Canada's largest-ever security breaches, a revelation that alarmed Five Eyes allies.

Cybersecurity firm executive pleads guilty to hacking hospitals

The former chief operating officer of a cybersecurity company pleaded guilty to hacking hospitals in June 2021 to boost his company's business. Vikas Singla, who worked for a security company that provided services to the healthcare industry, pleaded guilty to hacking into the systems of GMC Northside Hospital hospitals. During his attack he disrupted the health provider's phone and network printer services, and stole personal information of more than 200 patients.

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.

22/11/2023 – 2023–2030 Australian Cyber Security Strategy

21/11/2023 – LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability

9/11/2023 – CISA, NSA, and Partners Release New Guidance on Securing the Software Supply Chain

7/11/2023 – FEMA and CISA Release Joint Guidance on Planning Considerations for Cyber Incidents

Our Views:

New measures for improving national cyber resilience

Australia recently published its new cybersecurity strategy that articulates direction and key focus areas for 2023 to 2030. The strategy acknowledges how difficult it is for organisations to operate safely in the current global cyber-attack landscape and strongly signals a desire for Australia to adopt a leadership stance in cyber security. We look below at two issues outlined in the strategy that we believe are as relevant to the New Zealand organisations as they are to our friendly neighbours across the ditch.

1. Accessing Incident Response Advice and Support After a Cyber Incident

The ability to rapidly respond to a cyberthreat significantly improves an organisation's chance of minimising the impact of any incident. A rapid response also allows a quick return to business-as-usual activity. Unfortunately, many organisations struggle to gain timely support after an incident, making an already stressful situation, worse. The identified issues preventing easy access to cyber incident response advice and support include:

The need to report a cyber incident (either as a regulatory obligation or voluntarily) to multiple external agencies.

Not only does an organisation need to fully understand to who and how they report cyber incidents, the regulatory reporting processes can be a time-consuming distraction in the immediate aftermath of a severe incident. Additionally, agencies (such as New Zealand's Office of the Privacy Commissioner and Financial Markets Authority) will require timely and regular updates as to the status of any response. The New Zealand regulatory reporting requirements are currently less complicated than Australia's; however, they do exist. Others that may need to be notified include the NZ Police, CERT NZ as well as your commercial obligations including cyber insurers and customers. Additionally, many New Zealand organisations must comply with various industry and international regulations as they operate in a global marketplace making this an issue across Australasia.

Organisational reluctance to share information with government agencies, particularly the details surrounding any cyber incident or response, due to believing this may trigger a regulatory penalty or increased scrutiny.

The fear of sharing information makes it challenging for national agencies to assist organisations in the event of a cyber incident and seriously limits the ability for any national government to accurately understand or report on the current attack landscape.

Difficulty engaging private incident response services in a landscape of inconsistent industry service levels, and unclear professional standards.

National agencies have limited capacity and ability to support organisations during a cyber incident. Therefore, being able to access high quality, trusted and professional private incident response services is crucial to gain valuable support. Currently the industry is indicating a greater need for more professional and trusted incident response providers.

The Australian National Cybersecurity Strategy has outlined several new initiatives in response to the challenges identified above, as follows:

Firstly, they intend to appoint a national cyber coordinator to lead any government response during a major cyber incident. We believe this action broadly follows good practice incident management guidance such as that outlined in the Coordinated Incident Management System (CIMS) framework in New Zealand. Provided a clear RASCI is developed and understood across all of the public agencies responsible for crisis management and that this role is well-supported, it could provide a critical coordination point lacking in the environment to date.

Secondly, the Australian government indicate they will streamline incident reporting by developing a single regulatory reporting portal and furthermore investigate whether regulatory requirements can be streamlined. Streamlining legislation will benefit all by creating a less complicated environment. A single location to find information and see how and where to fulfil regulatory reporting obligations during a cyber incident is a valuable step. New Zealand would benefit from a similar national one stop location for cyber response assistance and information. We have available an automatic tool that generates notifications to agencies and communications to stakeholders to ensure reporting post incident are managed in a timely and efficient fashion.

The Australian Government intends to drive greater information sharing by "co-designing" a "limited use obligation" agreement. Essentially this is an agreement that will limit how their government agencies may use or share any information an organisation provides to them around a cyber incident. Note, this will not provide immunity from legal liability or law enforcement actions. We think this is an interesting idea and may go some way toward building trust between public and private entities in cyber and therefore allow national agencies to collect valuable data around the threat landscape. In regard to enabling better government support to organisations during a cyber incident, a greater government capacity and capability may be required in this area should the same levels of cyber activity continue. We believe that building stronger interpersonal relationships between external incident support resources and internal cyber resources within organisations is key. Developing trust through jointly planning, testing, and successfully executing response actions is ultimately a better way to drive more information sharing and achieve a more successful incident response.

Finally, the government intend to "co-design" an industry code of practice for incident response providers. This aims to grow confidence in cyber security professionals by clearly outlining quality and professional standards and expectations. Creating greater professionalism around all aspects of the cybersecurity industry is a positive move forward. As managing cyber risk is now critical, all cybersecurity practitioners should be held to an appropriate level of professional standards, similar or equivalent to those required by any other professional services industries. The New Zealand Government manage this process via the 'Marketplace' which involves a robust acceptance procedure.

In lieu of these standards we recommend you ensure confirming that any incident response provider you consider can demonstrate they have professional qualifications or certifications, show extensive experience in incident response, are following well renowned and tested cybersecurity and incident response frameworks (e.g NIST, SANS), and are using industry standard tools.

All the actions outlined by the Australian government are positive steps to improve incident response in Australia; however, it is crucial to note that they do not take any onus away from organisations who must be responsible for understanding that they have obligations to fulfil during a cyber incident and ensuring they have adequate additional support in place to fulfil these and guarantee the best outcome.

2. Pressure-testing critical infrastructure to identify vulnerabilities.

The strategy highlights how all organisations must be prepared to defend, respond to, and recover from major cyber incidents; however, it emphasises the vital nature of critical infrastructure to maintaining essential services. It therefore outlines a plan to increase national cyber readiness by using cyber security exercises and incident response plans to ensure vulnerabilities are identified and responses are tested.

The Australian government intend to conduct national cyber security exercises across all sectors to test a wide spectrum of incident response plans, measures, and communication channels. This will be led by the new national cyber coordinator role and involve exercising existing cyber incident response plans and processes to ensure they are adequate. It aims to identify vulnerabilities and possible improvements across industries. We believe if industry engage positively with the exercise, and it is run competently this could be a truly valuable action to significantly increase national cyber resilience. Our existing clients will understand how beneficial a cyber incident simulation can be to fast-track awareness of cyber risk within an organisation and quickly see where immediate cyber incident response improvements can be made. More recently we have been involved in simulations that involve organisations and third-party providers to test the communications and response flow across the ecosystem which is vital for an effective real-world response. We would like to see more of this activity in the New Zealand landscape and invite any industry or organisation keen to start improving and testing their response plans to contact us for assistance in arranging a cyber simulation exercise.

Finally, the national cyber coordinator in Australia intends to develop a series of "playbooks" for incident response. All organisations should at least have a basic set of playbooks in place for the most common cyber risk scenarios applicable to their businesses. National playbooks (as described in Australia's strategy) make sense as a starting point for guidance; however, each organisation must ensure they adopt tailored response playbooks that suit their unique context, data, systems, risk tolerance and resources.

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: