NZ Incident Response Bulletin

Standard Edition – June 2024 – Issue #65

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

MediaWorks hack: BreachForums site seized by FBI, international partners including NZ Police

The FBI, along with international partners including NZ Police, seized BreachForums, a hacker site that sold data stolen from MediaWorks. MediaWorks had data on 2.5 million Kiwis compromised, involving information from "The Block NZ" voters and competition entries. The site had been previously shut down and revived multiple times. MediaWorks confirmed no financial data or passwords were compromised. The FBI arrested site operator Conor Brian Fitzpatrick, who received a 20-year supervised release sentence.

New Zealand's NCSC briefs IPAC on potential cyber attacks

The New Zealand National Cyber Security Centre (NCSC) briefed the Inter-Parliamentary Alliance on China (IPAC) about potential cyber attacks targeting its members, likely by state-sponsored actors. Lisa Fong, Deputy Director-General of the GCSB, shared details of the NCSC's response and an internal review aimed at improving their procedures. The review findings will be made public by June 30, 2024. This underscores the ongoing threat landscape, with state-sponsored cyber attacks constituting a significant portion of incidents handled by the NCSC.

Australia

Cyber security chief says MediSecure data breach is an 'isolated' attack but warns health data a prime target for cybercrime

The MediSecure cyberattack, described by Australia's National Cyber Security Coordinator, Lieutenant General Michelle McGuinness, as an isolated ransomware incident, compromised personal and health data of individuals but did not impact current e-prescriptions or medication dispensing services. Originating likely through a third-party vendor, the breach triggered a swift governmental response involving multiple agencies to contain and investigate the extent of the damage. Although the full scale of the data compromised is still under review, authorities have reassured the public that there is no immediate need for affected individuals to replace their identification documents. This incident underscores the heightened vulnerability of the healthcare sector to cyber threats and the importance of robust cybersecurity measures.

Police investigate large-scale healthcare data breach at MediSecure

Federal police are investigating after Australian healthcare business MediSecure was targeted in a large-scale ransomware data breach. MediSecure's website and phone hotline were offline on Thursday, and the company confirmed in a statement it had fallen victim to a cyberattack. The Melbourne-based firm was founded in 2009 and provides electronic prescription services to healthcare professionals.

World

UK and allies unmask and sanction Russian leader of LockBit cybercrime gang

Britain, the US and Australia have sanctioned and unmasked a senior Russian leader of the notorious cybercrime gang LockBit. This action forms part of a broader effort to dismantle the group's operations, which involve ransomware attacks that encrypt victims' data and demand payment for its release. LockBit has been responsible for a significant number of global cyberattacks, targeting businesses and critical infrastructure. This coordinated move is part of a larger campaign against ransomware actors, emphasising the international community's commitment to combating cybercrime. The sanctions are intended to disrupt the gang's financial resources and hinder their ability to carry out further attacks. Additionally, law enforcement agencies, including the UK's National Crime Agency and the FBI, have been instrumental in this crackdown, leading to arrests and indictments of other LockBit members

UK engineering firm Arup falls victim to £20m deepfake scam

The British engineering company Arup has confirmed it was the victim of a deepfake fraud after an employee was duped into sending HK$200m (£20m) to criminals by an artificial intelligence-generated video call. Hong Kong police said in February that a worker at a then-unnamed company had been tricked into transferring vast sums by people on a hoax call "posing as senior officers of the company". Arup said in a statement that it was the company involved, confirming that at the beginning of the year it had "notified the police about an incident of fraud in Hong Kong". It confirmed that fake voices and images were used.

OAIC Statement on MediSecure data breach

The Office of the Australian Information Commissioner (OAIC) has been notified of the data breach involving MediSecure. The National Cyber Security Coordinator is working with agencies across the Australian Government, states and territories to coordinate a whole-of-government response to this incident. The OAIC is actively engaging and collaborating with other agencies in this process, with a particular focus on the privacy of individuals and their personal information. In accordance with our usual process, we have commenced preliminary inquiries with MediSecure to ensure compliance with the requirements of the Notifiable Data Breaches (NDB) scheme.

Under the NDB scheme, organisations covered by the Privacy Act 1988 must notify affected individuals and the OAIC as soon as practicable if they experience a data breach that is likely to result in serious harm to individuals whose personal information is involved. As information about a data breach is gathered and assessed, the initial focus for the OAIC is ensuring that affected individuals are appropriately informed, so they may take steps to protect themselves from any further risk to their personal information.

US pharma giant Cencora says Americans' health information stolen in data breach

U.S. pharmaceutical giant Cencora says it is notifying affected individuals that their personal and highly sensitive medical information was stolen during a cyberattack and data breach earlier this year. In letters to affected individuals sent out this week, Cencora said that the data from its systems includes patient names, their postal address and date of birth, as well as information about their health diagnoses and medications.

The pharma giant said it had initially obtained patients' data through partnerships with the drug makers it works with "in connection with its patient support programs." That includes patients of AbbVie, Acadia, Bayer, Novartis, Regeneron, and other companies. Cencora has not yet described the nature of the cyberattack, which began on February 21 and was not publicly disclosed until the company filed notice with government regulators a week later on February 27. The company, known as AmerisourceBergen until 2023, handles around 20% of the pharmaceuticals sold and distributed throughout the United States.

GitHub flaw raises alarm over supply chain security risks

A recently uncovered vulnerability in GitHub Enterprise Server (GHES) has precipitated warnings from industry experts about the increasing threat of supply chain attacks. The issue, potentially allowing attackers to bypass authentication, has sparked concerns among cybersecurity professionals, emphasising the critical need for timely software updates.

Nick Mistry, Senior Vice President and Chief Information Security Officer at Lineaje, highlighted the severe risks posed by this vulnerability. Mistry stressed that organisations must swiftly address the patch to avoid substantial damage. "If not addressed promptly, an attacker could exploit this vulnerability to gain unauthorised access to important code repositories and related systems by evading authentication and taking control of administrative functions," Mistry stated. He further noted that the integrity and security of software products could be compromised, leading to malicious code introduction, theft of confidential information, and disruption of development processes.

Nissan A/NZ's outsourced cyber incident call centre breached

Nissan Australia and New Zealand faced a data breach involving their outsourced cyber incident call center managed by P&N Group. This breach exposed personal information of individuals who contacted Nissan for cyber-related issues, including names, contact details, and specific queries about the incidents. Nissan has assured that no financial information was compromised and is working with P&N Group to enhance security measures and support affected customers.

UK watchdog looking into Microsoft AI taking screenshots

The UK Information Commissioner's Office (ICO) is investigating Microsoft's new feature, Recall, which captures and stores encrypted screenshots on its upcoming Copilot+ PCs. Recall takes screenshots every few seconds and stores them locally on the user's device, with the capability to search through past activities including files, photos, emails, and browsing history. Microsoft assures that this feature is optional, and users can control what is captured and limit access to these snapshots.

Privacy advocates, however, express significant concerns, labelling Recall a potential "privacy nightmare." They worry about the chilling effect on user behaviour, as constant screenshotting could deter individuals from accessing confidential or sensitive information. Microsoft insists that Recall is designed with privacy in mind, allowing users to exclude certain websites and ensuring that private browsing in its Edge browser is not captured. The company emphasises that the data is not accessible to Microsoft or external parties without device access.

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.

9/05/2024 - Choosing Secure and Verifiable Technologies

Our Views:

Cyber Governance – Getting Started

What is Cyber Governance?

Cyber governance refers to the comprehensive approach an organisation takes to manage cyber risk. It involves establishing and maintaining a framework, along with supporting management structures and processes to ensure that cybersecurity strategies align with business objectives. Cyber governance activities include establishing decision-making hierarchies and accountability frameworks, setting expectations for risk appetite and tolerance, establishing oversight processes and procedures, and complying with applicable laws and regulations through adherence to policies and internal controls. In essence, cyber governance is a key mechanism through which a business can achieve cyber resilience.

While we have previously written on this topic, we are seeing an increasing number of client enquiries asking how to properly get started and make good progress.

The National Cyber Security Centre (NCSC) outline six key steps that businesses can focus on to improve their cybersecurity governance. The steps include:

1. Building a Cybersecurity Culture
2. Establishing Roles and Responsibilities
3. Holistic Risk Management
4. Organisational Collaboration
5. Creating a Cybersecurity Programme
6. Measuring Cybersecurity Resilience

Establishing effective cyber governance takes dedicated effort and as seen in the steps above, it encompasses a wide variety of leadership, cultural, procedural, and technological areas. However, getting started does not need to be difficult and we recommend the use of proven policy and plan templates and straightforward self-assessments to simplify this journey.

Why is Cyber Governance Important?

Cyber governance is crucial for several reasons. As cyber risks grow, there is increased concern and scrutiny on companies' cybersecurity practices from customers, suppliers, investors, regulators, and other stakeholders. Implementing strong cyber governance demonstrates an organisation's preparedness, resilience, and response capability to cybersecurity incidents and helps to build trust and ensure regulatory compliance. Effective cyber governance will also help mitigate the risks of data breaches, enable faster response to incidents, and provide a better understanding and adaptation to new cyber threats. Additionally, cyber governance aligns cybersecurity measures with business objectives, ensuring that security initiatives support and facilitate the overall mission of the organisation.

How do I start implementing Cyber Governance?

We recommend organisations start their cyber governance journey by gaining a good understanding of their current state. For example: What information is held and needs to be protected? What security measures are already in place? What are your critical business assets? Secondly establishing a cyber security programme that utilises a well-recognised industry framework and set of controls to address the risks identified in your business is essential.

If your business is either at the beginning of the journey or making to look improvements to cyber resilience, we advise completing a self-assessment against the CIS Critical Security Controls (CIS Controls) to enable you to identify key risks, areas of weaknesses, and easy improvements for immediate security uplift. The CIS Controls are a prescriptive, highly prioritised, and simplified set of best practices that can be used to strengthen your organisational cybersecurity posture. As many successful cyber-attacks exploit poor cyber hygiene such as inadequate configuration management, unpatched software, or lack of employee awareness, the implementation of basic security hygiene controls can significantly reduce your organisations cyber risk.

When starting we advise you to:

1. Understand your target state: The CIS controls allow you to choose an appropriate target cyber maturity level for your organisation, so all actions undertaken are appropriate for your unique business profile.
2. Start small: An effective cybersecurity improvement program must be realistic and achievable for your business. If resources are scarce, it is important to focus on steady and consistent small lifts in maturity. A roadmap that clearly articulates what, when, who and how the initiatives will be delivered is key to managing this process. Any plan should be evaluated at least quarterly and adjusted based on progress and ability.
3. Use strong prioritisation: Rather than attempting to implement every cybersecurity recommendation published which can result in unnecessary spend and overwhelm, ensure you are prioritising improvement activities that protect against the latest active attacks in the cyber landscape and those which reflect your organisations greatest risk areas.

By adopting a structured cybersecurity framework, you can begin your cyber governance journey with confidence and start implementing measurable uplifts to your cybersecurity to reduce your unique cyber risk.

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: