NZ Incident Response Bulletin

Premium Edition – November 2023 – Issue #58

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

Taumata Rau Conversation pushes cybersecurity up the agenda

Two years ago, the Royal Commission of Inquiry into a terrorist attack in Christchurch challenged the government to build a conversation with New Zealanders about national security challenges. An expert discussion on cybersecurity at the University on 24 October was a contribution to that goal. "We need the sorts of conversations that we're having now," Tony Lynch, a top national security official, told the audience. Fellow panellists in the Taumata Rau Conversation, hosted by Vice-Chancellor Professor Dawn Freshwater, were:

- Professor Giovanni Russello, the head of the University's School of Computer Science
- Lisa Fong, deputy director-general, National Cyber Security Centre
- Amber McEwen, the chief executive officer of Research Education Advanced Network New Zealand

The background included cyber-attacks which have targeted nationally significant organisations including Parliament and universities. A ransomware assault crippled the Waikato District Health Board in 2021 and last month electronic ticketing for Auckland public transport was similarly taken out of action. Lynch, the head of the National Security Group in the Department of the Prime Minister and Cabinet, walked the audience through the nation's first national security strategy Secure Together - Tō Tātou Korowai Manaaki, issued in August by the Ministry of Defence.

FMA Reinforces Importance of Cyber-resilience For Financial Service Providers

The Financial Markets Authority (FMA) – Te Mana Tātai Hokohoko – is reminding licensed financial service providers about the importance of cyber-resilience as part of Cyber Smart Week 2023. CERT NZ has also launched a new website for New Zealanders to stay secure online called Own Your Online.

As part of the FMA's role in promoting fair, efficient, and transparent markets, we encourage all financial service providers to protect themselves online, particularly with the growing threat from online scams and data attacks. Effective management of cyber risk by financial service providers directly contributes to the operational resilience capability of the entity. One of the requirements for some FMA-licensed entities is that they must notify the FMA of any event that materially impacts the information security of their critical technology systems, which can be caused by cyber-related incidents.

A 2019 thematic review of cyber resilience in FMA-regulated entities found most participants were aware of the increasing cyber security risk and assessed themselves as being highly capable of protecting against, and recovering from, such threats. However, participating entities did not rate themselves highly in terms of detecting and responding to cyber threats. Participants also predicted that their cyber resilience was generally expected to improve over the following two years.

MBIE expands intelligence spy unit MI beyond immigration

The government's super-ministry has quietly embedded itself in the country's spy agency network, more than tripling the size and spending of its own powered-up intelligence-gathering arm. Newly released Official Information Act documents show the Ministry of Business, Innovation and Employment's (MBIE) intelligence wing, MI, has expanded in the past 12 months beyond immigration to cover the entire sprawling ministry, taking charge of intelligence and operations if there is a national security threat. Its budget has doubled in one year to $11 million - almost quadruple what it was in 2017 - and its staff has grown to 115.

Its focus is on "national security and intelligence" through a "National Security Intelligence Team", even though the New Zealand Security Intelligence Service (SIS), Government Communications Security Bureau (GCSB) and National Assessment Bureau already do this. Unlike MI, those spy agencies all have outside scrutiny from an independent watchdog; MI has none, only an internal monitoring group.

World

SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures

The Securities and Exchange Commission announced charges against Austin, Texas-based software company SolarWinds Corporation and its chief information security officer, Timothy Brown, for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. The complaint alleges that, from at least its October 2018 initial public offering through at least its December 2020 announcement that it was the target of a massive, nearly two-year long cyberattack, dubbed "SUNBURST," SolarWinds and Brown defrauded investors by overstating SolarWinds' cybersecurity practices and understating or failing to disclose known risks. In its filings with the SEC during this period, SolarWinds allegedly misled investors by disclosing only generic and hypothetical risks at a time when the company and Brown knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time.

As the complaint alleges, SolarWinds' public statements about its cybersecurity practices and risks were at odds with its internal assessments, including a 2018 presentation prepared by a company engineer and shared internally, including with Brown, that SolarWinds' remote access set-up was "not very secure" and that someone exploiting the vulnerability "can basically do whatever without us detecting it until it's too late," which could lead to "major reputation and financial loss" for SolarWinds. Similarly, as alleged in the SEC's complaint, 2018 and 2019 presentations by Brown stated, respectively, that the "current state of security leaves us in a very vulnerable state for our critical assets" and that "[a]ccess and privilege to critical systems/data is inappropriate."

The SEC's complaint alleges that Brown was aware of SolarWinds' cybersecurity risks and vulnerabilities but failed to resolve the issues or, at times, sufficiently raise them further within the company. As a result of these lapses, the company allegedly also could not provide reasonable assurances that its most valuable assets, including its flagship Orion product, were adequately protected. SolarWinds made an incomplete disclosure about the SUNBURST attack in a December 14, 2020, Form 8-K filing, following which its stock price dropped approximately 25 percent over the next two days and approximately 35 percent by the end of the month.

British Library suffering major technology outage after cyber-attack

The British Library is suffering a technology outage after it was hit by a cyber-attack, which is affecting services online and its sites in London and Yorkshire. Access to the website, as well as the catalogue and digital collections, is temporarily unavailable. The collection of items ordered on or after 27 October, new collection item orders via digital catalogues and reading room PCs are also inaccessible, it said. Reader registration is also unavailable. The British Library said on Tuesday it had launched an investigation into the incident with the support of the National Cyber Security Centre (NCSC) and other cybersecurity specialists. A statement said: "The British Library is experiencing a major technology outage, as a result of a cyber incident. This is affecting online systems and services, our website, and onsite services including our reading rooms. We are investigating the incident with the support of the National Cyber Security Centre (NCSC) and cybersecurity specialists."

Boeing assessing Lockbit hacking gang threat of sensitive data leak

Boeing Co said it was assessing a claim made by the Lockbit cybercrime gang that it had "a tremendous amount" of sensitive data stolen from the aerospace giant that it would dump online if Boeing didn't pay a ransom. The hacking group posted a countdown clock on its data leak website with a message saying, "Sensitive data was exfiltrated and ready to be published if Boeing do not contact within the deadline! For now we will not send lists or samples to protect the company BUT we will not keep it like that until the deadline," the hacking group said. The hacking group typically deploys ransomware on a victim organization's system to lock it up and also steals sensitive data for extortion.

"We are assessing this claim," a Boeing spokeswoman said by email. Lockbit was the most active global ransomware group last year based on the number of victims it claimed on its data leak blog, according to the U.S. Cybersecurity and Infrastructure Security Agency (CISA).

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.

9/11/2023 – 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

Spotlight topics:

Australian Information Security Association Conference 2023

As digital forensic incident response (DFIR) and cyber specialists, attendance at such events ensures we remain across the latest technology and risk developments. Following the travel restrictions of recent years, we attended several international industry events, including Open Text World in Las Vegas and the Techno Security & Digital Forensics Conference in San Diego during 2022. October 2023 marked the first occasion that Incident Response Solutions attended the Australian Information Security Association (AISA) Conference.

We consider that attendance of an AISA Cyber Conference in Australia should be on the wish list for New Zealand cyber practitioners given its proximity to New Zealand, and breadth of learning and networking opportunities. At this year's event, there was an unprecedented record attendance of around 5,500 registrants, 34 learning streams, 439 Speakers, 405 Speaker Sessions, 150 Exhibitors, a CISO Boot Camp, 59 Think Tanks and 16 Workshops across three days, along with a closing keynote from Professor Brian Cox about our universe, which is not to be forgotten.

Delegates ranged from company directors and managers to public servants, lawyers, risk and privacy professionals, software architects and technical security specialists from a broad range of industries such as education, finance, government, healthcare, manufacturing, mining, transportation and utilities.

Key takeaways

We attended a range of speaking sessions including Cyber Governance, Security Risk Management, Incident Response, Legal and Privacy issues amongst many others. The ample breaks in between these sessions provided an opportunity to either reconnect with Australian colleagues or meet new experts and discuss the changing landscape. Given the recent high-profile breaches in Australia, it was clear that there is an increasing awareness of the risks associated with cyber-attacks, and a genuine desire to do better.

With so many exhibitors on site, we were able to wander the hall and have valuable discussions with the representatives at chosen booths. We found the insights provided by vendors who offer advance threat detection and response capabilities, along with those who provide solutions to the CIS Controls such as password managers, access control, data recover, security training and supply chain management were particularly useful.

A recurring theme across the sessions attended was the interconnect between Cyber Governance and Resilience. The message which cyber experts have been extolling for many years is now loud and clear that organisations should have a cyber strategy, adopt a set of controls, continually monitor the threat landscape, have an incident response plan and regularly practice this via simulations. These are the services that Incident Response Solutions founded as a specialist business five years ago now to meet the growing requirements of New Zealand businesses. During 2023, we have seen an increase in demand for our services from Australian business, which we are pleased to be able to remotely assist with from our Auckland base.

The end of each day provided a great opportunity to unwind with fellow practitioners from both New Zealand and Australia and discuss recent events and the road ahead. We are grateful for the opportunity that the conference provided in bringing so many of Australia's leading experts into the fantastic hub in Melbourne where we could network and depart with so many exciting opportunities to work together on the horizon.

I would highly recommend any New Zealand practitioners looking to expand their cyber knowledge to consider attending an upcoming event. Compared to the options available in the United States, this conference was much closer to travel to, had a Australasian focus, and had very reasonably priced admission and accommodation fees where the more favourable exchange rate didn't have as much affect as the $18 coffees being purchased in the US.

Following on from the conference, we also met with a number of companies in Melbourne and Sydney. Highlights included meetings with companies operating in the field of Law, Public Relations, Insurance, Cyber Security, as well as several of our key DFIR vendors including Nuix and Reveal.

Our Views:

Improving cybersecurity when you have limited resources

Threats to your technology such as information theft, phishing, ransomware, denial of service, website defacement, and even natural disasters are regularly impacting organisations of all sizes and maturity. Not even the largest and most well-equipped businesses are immune. There are well-known strategies that can be used to defend against all of these threats however they are not always undertaken, especially by smaller or less well-resourced organisations who may believe they require greater budgets or more skills before attempting to implement security controls.

We believe any action is better than none however and therefore we suggest following a new guide from the Centre for Internet Security (CIS). The guide lays out a simple step by step process that is designed to assist organisations who have small budgets and limited staff successfully progress towards implementing the essential security hygiene controls. The process consists of six phases that are designed to ensure you fully understand your IT environment and that you can confidently answer the following questions:

- What computers, phones, and other IT assets are being used in your office?
- Are you using unique, secure passwords and multi-factor authentication wherever possible?
- Are your computers set up with security in mind?
- Do you manage who has extra privileges on your network or access to sensitive information?
- Are your staff clear about their role in protecting your enterprise from cyber incidents?

Phase 1 – Identification and Inventory

This phase involves completing five worksheets that allow you to inventory exactly what you have in your organisation to protect. Understanding this is essential because if you are unclear of your assets, you may not protect them all. Each worksheet may take 2-4 hours to complete on first attempt, however updating these sheets moving forward is a much quicker task and you should aim to update these sheets regularly. As the completed worksheets will hold sensitive information about your priority assets it is important these are protected whether you choose to save them electronically or physically.

- Enterprise Asset Inventory Worksheet
    a. Create an Enterprise Asset Management Policy (CIS Enterprise Asset Management Policy Template).
    b. Complete the Enterprise Asset Inventory Worksheet (Enterprise Asset Inventory Worksheet).
    c. To see all devices connected to your network you can check your wireless router internet protocol (IP) address and device names. If you have a larger network, consider investigating commercial or opensource network scanning tools.

- Software Asset Inventory Worksheet
    a. Create a Software Asset Management Policy (CIS Software Asset Management Policy Template).
    b. Complete the Software Asset Inventory Worksheet (Software Asset Inventory Worksheet).
    c. To help create an inventory of application running on your computers you can manually check the installed programs with the operating system and periodically check what applications are running on your devices using auditing tools.

- Data Inventory Worksheet.
    a. Create a Data Management (CIS Data Management Policy Template) and Audit Log Management Policy (CIS Audit Log Management Policy Template).
    b. Complete the Data Inventory Worksheet (CIS Data Inventory Worksheet).
    c. Examples of data you should identify includes Credit card, banking, other financial data, Personally Identifiable Information (PII), names, birthdates, addresses, medical data, usernames, passwords, customer lists, trade secrets, Intellectual Property.
    d. Ensure you are familiar with any regulatory requirements that you need to comply with.

- Service Provider Inventory Worksheet
    a. Create a Service Provider Management Policy (CIS Service Provider Management Policy Template).
    b. Complete the Service Provider Inventory Worksheet (Service Provider Inventory Worksheet).
    c. Add web services and cloud solutions to your inventory.
    d. Check with your team to identify any additional filesharing or online platforms they use.

- Account Inventory Worksheet
    a. Create an Account Management Policy (Account and Credential Management Policy Template).
    b. Complete the Account Inventory Worksheet (Account Inventory Worksheet).
    c. Check with your team to identify further websites and services they use for work and hold accounts for.

Phase 2 – Secure Configuration

The second phase of this process is securely configuring each of your devices and completing the asset protection worksheet for all assets on your inventory. To complete this you should:

- Define policies for secure configuration, malware defence and vulnerability management. (CIS Secure Configuration Management Policy Template), (CIS Malware Defense Policy Template), (CIS Vulnerability Management Policy Template).
- Complete an Asset Protection Worksheet for every device listed in your asset inventory. (Asset Protection Worksheet)
- Have a look at using CIS benchmarks for securing systems that process the most sensitive data.

Phase 3 – Account Security

This phase secures the accounts you have listed in your account inventory and involves:

- Ensuring you have an account management policy (Account and Credential Management Policy Template).
- Completing the Account Security Worksheet for each account listed in your inventory (Account Security Worksheet).
- Passwords should be unique, 14 characters or more and include at least 1 special character. MFA or 2FA should be enabled for all services where possible. Use admin accounts only for necessary admin activity. Educate your team on secure credentials.

Phase 4 – Backup and Recover

Phase 4 creates backups for all your sensitive data which is one of the best ways to protect your organisation and enable recovery after a cyber incident.

- Define a policy for data recovery (CIS Data Recovery Policy Template).
- Complete a Backup and Recovery Worksheet for ever asset in your organisation. (Backup and Recovery Worksheet)
- Don't forget paper assets and ensure at least one backup destination is offline.
- Test your backups regularly.

Phase 5 – Incident Response

This phase prepares you with a plan to follow in the event of a cyber incident. To be prepared you should:

- Create a policy for incident response management. (CIS Incident Response Policy Template)
- Complete the Incident Response Worksheet. (Incident Response Worksheet)
- Practice and test your plan.

Phase 6 – Train your Team

Cyber Security is all about people! Strong cybersecurity awareness is key to remaining secure. This phase is completed by:

- Developing a policy for cybersecurity awareness training. (CIS Security Awareness Skills Training Policy Template)
- Complete the Cyber Education Worksheet. (Cyber Education Worksheet template)

Our key tips for making progress:

While we see the enormous value of creating organisational policies in defining your risk appetite and clearly articulating your goals and expectations to all team members, this step should not stall your progress. If the creation of approved policies is taking too long or stalled, then please continue through the process, and start completing the inventory worksheets in parallel.

Do not let the drive for perfection in any of these activities slow or prevent progress. Dedicating 10 minutes a day will see results. If you follow the steps, you will be in a more secure position.

Utilise the free tools, worksheets, and advice.

Ask for help. We are more than happy to help you progress in any of these activities should you need a bit more advice or just a resource to draft your positions.

If you wish to know more around implementing cyber governance and ensuring your cybersecurity investments are well planned and managed, please contact us. We look forward to assisting you achieve your cybersecurity goals and maximise your cybersecurity investment.

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: