NZ Incident Response Bulletin

Standard Edition – June 2022 – Issue #41

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

Spies, cyberattack initiatives get more money in Budget 2022

Spy agencies and counter-terrorism initiatives will get millions more in funding after Budget 2022. Signals intelligence agency the GCSB will get nearly $50 million more funding over four years to combat cyberattacks and engage in more counter-terrorism activity. The agency will receive $14.3 million more in additional funding over four years, plus another $19 million for maintaining and enhancing cybersecurity services. The new cybersecurity initiative aims to protect information services "from the increasing frequency and severity of cyberattacks". The bureau will also get $12.6 million over four years to enhance counter-terrorism services. This initiative is in response to suggestions from the Royal Commission of Inquiry into the Christchurch mosque attacks.

$3.7m lost to cyber scams in first quarter

Cyber scams are continuing to evolve, with urgency, fear and opportunity used to dupe victims into parting with their money. CERT NZ's Cyber Security Insights report for the first quarter of the year indicates the number of cyber incidents and the associated financial losses have dropped back a bit from the last quarter of 2021 but were still high. "The previous quarter saw a spike due to the prevalent Flubot campaign, which used text messages to install malicious malware on New Zealanders' devices," CERT director Rob Pope said.

CERT received 2,333 reports in the three months ended March 2022, which was an increase of 63 percent from the same quarter last year. There were direct financial losses of $3.7 million, which was up 23 percent on the year earlier. Phishing and credential harvesting made up 59 percent of all reports.

Pope said phishing had been around for decades but had evolved over that time. He said scammers often stole people's personal credentials to gain unauthorised access to accounts and systems, which could provide a gateway to other scams. "Attackers change their tactics to reflect current events and use social engineering triggers, like urgency, fear and opportunity," he said. "Phishing is a major concern as it's simple to do, from a technical perspective, and it's a gateway to other kinds of incidents."

Interview with NCSC Director Lisa Fong at CYBERUK 2022

Lisa Fong, Director of the New Zealand's GCSB National Cyber Security Centre, represented the organisation at the United Kingdom Government's premier cyber security conference, CYBERUK 2022. One of Lisa's engagements at CYBERUK 2022 was an interview with the NCSC-UK's Director of Communications, James Stewart, covering the NCSC's work to help protect New Zealand's critical national infrastructure. She provided a New Zealand perspective on the cyber threats many organisations are facing, including supply chain vulnerabilities and ransomware. She also spoke about the importance of diversity in the workforce and highlighted the GCSB's ongoing focus in this area.

TupuToa and Microsoft partner to boost Māori and Pacific diversity in cybersecurity

Microsoft and TupuToa, a social enterprise focused on growing Māori and Pacific leaders in Aotearoa, have announced a new partnership that aims to create more diversity in the country's cybersecurity sector. The deals will see TupuToa and the US technology giant working together to co-develop a cybersecurity employment program aiming to build new career pathways. New Zealand was one of 23 countries selected by Microsoft to receive funding under a global initiative targeted at closing the cybersecurity skills gap, recognising the increased risk to local businesses from cyber threats as well as the need to address diversity within the cybersecurity industry.

World

Cybersecurity rulings important for all Australian businesses

The world of cybersecurity is overflowing with principles. Principles about patching, passwords and people. Principles about physical security, phishing and firewalls. However, until recently, there has been little legal precedent supporting these principles and without such precedent, principles can be difficult to enforce. The past month has served up two landmark cases that will help establish a new level of precedent for cybersecurity in Australia - one in the Federal Court and one in the ACT Civil and Administrative Tribunal. Both cases deserve utmost attention from senior management, boards and directors as our nation navigates a new era of cybersecurity uplift. These cases should not be dismissed as just technical 'principles'.

US offers $15M for info on Conti ransomware

The U.S. Department of State set two separate bounties for information on the Conti ransomware organized crime group totalling $15 million USD. Any information that helps identify or locate the Conti group leaders will be awarded up to $10 million. Additionally, $5 million will be awarded for any information that leads to the arrest of individuals conspiring with the Conti group. The rewards are offered under the Department of State's Transnational Organized Crime Rewards Program and can be claimed from any country.

Near $1 Million Fine Proposed for Colonial Pipeline Following Cyber Attack

A near $1 million penalty is being proposed for Colonial Pipeline following widespread fuel shortages along the U.S. East Coast in 2021 after a cyber-attack on the energy pipeline operator in May 2021. The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration found management failings and has issued a Notice of Probable Violation and Proposed Compliance Order to Colonial Pipeline Company, which includes multiple probable violations of Federal pipeline safety regulations. The proposed civil penalties amount to $986,400.

On May 8, 2021, Colonial Pipeline confirmed that its information technology systems were compromised by a ransomware attack. As a precaution, Colonial temporarily halted operational technology functions across four of its mainlines that transport gasoline, diesel, and jet fuel, stretching from Texas to New Jersey. The attack resulted in major fuel distribution shortages across the region that the Colonial pipeline serves, which led to 17 states declaring states of emergency relative to the shortages.

Anonymous Leak 82GB of Police Emails Against Australia's Offshore Detention

In total, Anonymous leaked 285,635 confidential emails belonging to the Nauru Police Force. According to Anonymous, the data leak was in protest against the alleged ill-treatment of asylum seekers and refugees carried out by Island authorities on behalf of the Australian government. As seen by Hackread.com, the total number of leaked emails is 285,635 and available for direct and torrent download through the official website of "Enlace Hacktivista," a platform that aims to "Document hacker history."

Cyber security: Global food supply chain at risk from malicious hackers

Modern "smart" farm machinery is vulnerable to malicious hackers, leaving global supply chains exposed to risk, experts are warning. It is feared hackers could exploit flaws in agricultural hardware used to plant and harvest crops. Agricultural manufacturing giant John Deere says it is now working to fix any weak spots in its software. A recent University of Cambridge report said automatic crop sprayers, drones and robotic harvesters could be hacked. The UK government and the FBI have warned that the threat of cyber-attacks is growing. John Deere said protecting customers, their machines and their data was a "top priority".

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 our YouTube Channel and this webpage.

Alerts

18 May 2022 - NCSC - Weak security controls and practices routinely exploited for initial access

11 May 2022 - CISA - Protecting Against Cyber Threats to Managed Service Providers and their Customers

News Clips

11 May 2022 - Interview with NCSC Director Lisa Fong at CYBERUK 2022

Our Views:

Cyber Security Awareness – Practical Tips to Protect Your Systems

Introduction

So far during the second quarter of 2022, we have seen an alarming increase in the number of New Zealand organisations falling victim to Email Phishing attacks. These attacks not only attempt to steal your login credentials, but also trick you into running malicious software that will then be used by the attackers to conduct data theft, ransomware and more.

It is therefore more important than ever to ensure that your staff understand the wide variety of cyber security risks your organisation faces. At Incident Response Solutions, we believe cyber security risks are best mitigated by following an evidence-based approach; what are the local incident response firms responding to most often, what does current data breach research tell us, and what cyber security controls should be applied based on those findings?

According to the 15th annual Verizon Data Breach Investigations report, published this month, 82% of breaches involved the Human Element, including Social Attacks, Errors and Misuse. The four key paths leading to a breach of your systems include attackers using stolen credentials, conducting phishing attempts, exploiting software vulnerabilities and running botnets. The report concludes organisations must have a plan to handle these risks.

To improve your organisation security, we recommend conducting a four-pronged cyber security awareness campaign:

Step 1 – Credential Monitoring

Scan your domain name for any instances of compromised credentials across your organisation and demonstrate to staff how their passwords can easily be obtained and reused by attackers. Note that you also have obligations under the new Privacy Act 2020 in relation to data breaches that may result in serious harm. We recommend changing all valid passwords located immediately upon discovery of using this service.

Step 2 – Phishing Simulation

A Phishing simulation is a training tool that organisations can use to send realistic phishing email to employees in order to test their level of awareness of such attacks, as well as advising them on what to do with phishing emails when they receive them. We recommend you run a carefully planned set of simulated phishing attacks to help you find out how vigilant your employees are and how they can be trained further. The effectiveness of these simulations is more effective if you customise the phishing kits so it contains text and formatting from a third party that your staff often communicate with.

Step 3 – Online Cyber Training and Awareness

The Verizon report emphasises the need to increase staffs' awareness of what tactics attackers are likely to use against organisations, specific to your industry, both as a tool to encourage executives to support much needed security initiatives and as a way to illustrate to employees the importance of security. The report suggests that on average, staff at organisations that run online training spend around one hour per year.

We believe that every dollar spent on cyber security awareness training significantly reduces your organisation's vulnerability to cyberattacks. Doing this not only helps you save thousands of dollars in the event of a breach but could prove to be priceless when avoiding long-term costs such as lost customer trust and damage to your reputation.

Step 4 – Cyber Security Controls

The above three steps form the foundation for improved cyber security awareness. However, we recommend going one step further and formalising your cyber security awareness programme under a recognised set of Cyber Security Controls. We recommend the Centre for Internet Security (CIS) Controls. The 18 controls define basic cyber hygiene and represents a minimum standard of information security for all enterprises. At implementation group level 1 (out of 3), enterprises with limited cybersecurity expertise can thwart general, non-targeted attacks. Control 14 deals with Security Awareness and Skills Training, including the following safeguards:

- 14.1 Establish and Maintain a Security Awareness Program
- 14.2 Train Workforce Members to Recognize Social Engineering Attacks
- 14.3 Train Workforce Members on Authentication Best Practices
- 14.4 Train Workforce on Data Handling Best Practices
- 14.5 Train Workforce Members on Causes of Unintentional Data Exposure
- 14.6 Train Workforce Members on Recognizing and Reporting Security Incidents
- 14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
- 14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks

It is noteworthy that at implementation group level 1, there are 56 possible safeguards (or sub-controls) across the 18 controls, and that 8 of the 56 are attributed to Security Awareness and Skills Training. We can assist you with all four steps detailed above.

NZ Incident Response Bulletin

Standard Edition – June 2022 – Issue #41

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: