NZ Incident Response Bulletin

Standard Edition – November 2024 – Issue #70

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

Teen arrested for 'smishing scam' using technology never before seen in New Zealand

In October 2024, a 19-year-old in New Zealand was arrested for a sophisticated "smishing" scam, using an SMS Blaster device previously unseen in the country. This device acted as a fake cell tower, tricking nearby cell phones into connecting to it and then sending scam messages posing as banks to gather personal information. A multi-agency investigation, including the Department of Internal Affairs and Australia's cybercrime team, disrupted the scheme before financial losses occurred, although about 120 people were targeted. The suspect faces charges of interfering with a computer system and will appear in court in December.

Five Eyes alliance gives security guidance for tech start-ups

The Five Eyes alliance recently released security guidance for tech start-ups to counter economic espionage risks. This initiative follows a summit between intelligence agencies from New Zealand, Australia, Canada, the UK, and the US with the tech sector in Silicon Valley. The report, titled "Secure Innovation," provides practical measures for start-ups to integrate security into their operations, ensuring protection without stifling innovation. According to New Zealand's SIS Director-General, Andrew Hampton, some foreign states actively attempt to steal emerging tech, particularly those with military applications, via in-person or cyber spying, underlining the importance of robust security from the outset.

The guidance includes five principles: understanding threats, securing the business environment, integrating security into products, safeguarding partnerships, and managing risks during growth. By implementing these practices, start-ups not only protect their intellectual property but also enhance their appeal to investors. Minister Judith Collins emphasized the non-benign environment start-ups face, highlighting the potential for state and criminal actors to exploit technological advancements. By prioritising security, start-ups can foster resilience and potentially gain a competitive advantage in the marketplace.

Google says it will stop linking to New Zealand news if proposed new law passed

In October 2024, Google announced that it would stop linking to New Zealand news content if New Zealand's government passed a proposed law requiring large tech platforms to compensate news publishers for displaying or linking to their articles. The legislation aims to ensure fair compensation for local media by redistributing a portion of digital advertising revenue. Google raised concerns that such a law would compel it to modify its service offerings significantly, potentially affecting how it operates in New Zealand. The company pointed to similar laws in other countries, suggesting that mandatory payments could make it unsustainable to continue offering certain free services.

NZ officials silent on questions over Temu and cybersecurity

New Zealand's National Cyber Security Centre (NCSC) advised New Zealanders to remain vigilant with foreign apps, as overseas data laws could still apply. The agency's response has raised concerns about data security as apps like Temu gain popularity locally, highlighting the tension between consumer choice and national security.

Australia

Government introduces landmark cyber security legislation

The Australian Government introduced the Cyber Security Legislative Package 2024, aiming to enhance national cybersecurity measures. Key components include:

- Mandatory Ransomware Payment Reporting: Certain businesses are now required to report ransom payments to authorities.
- Minimum Security Standards for Smart Devices: Establishing baseline cybersecurity standards for smart devices to protect consumers.
- Limited Use Obligations: Imposing restrictions on how the National Cyber Security Coordinator and the Australian Signals Directorate can use information shared by businesses.
- Cyber Incident Review Board: Establishing a board to analyse significant cyber incidents and provide recommendations.

These measures aim to align Australia with international best practices and strengthen its position as a global leader in cybersecurity.

World

Marriott Pays $52M to Settle US States' Breach Litigation

Marriott has agreed to pay $52 million to settle litigation with U.S. states following a major data breach that exposed millions of customers' personal information. The breach, which occurred over several years, involved unauthorized access to the reservation system of its Starwood subsidiary, affecting information such as credit card numbers and passport details. This settlement resolves claims from multiple states that Marriott did not adequately secure its systems or respond quickly enough to protect customer data, a response that state officials argued failed to meet required data protection standards. The funds from the settlement will be directed to enhance consumer protection and cybersecurity programs across the affected states.

International Counter Ransomware Initiative 2024 Joint Statement

In October 2024, the International Counter Ransomware Initiative (CRI) convened its fourth gathering in Washington, D.C., with 68 member nations, including New Zealand, to enhance global resilience against ransomware threats. The CRI welcomed 18 new members and reaffirmed commitments to collective defense strategies, such as developing secure software standards, countering the misuse of virtual assets, and collaborating with the private sector. Key initiatives included the establishment of information-sharing platforms, the creation of a Public-Private Sector Advisory Panel led by Canada, and discussions on leveraging artificial intelligence to combat ransomware. These efforts aim to disrupt the ransomware ecosystem and hold perpetrators accountable.

Microsoft said it lost weeks of security logs for its customers’ cloud products

Microsoft has acknowledged a significant lapse in its cloud services, revealing that a bug caused the loss of over two weeks' worth of security logs for customers using platforms like Microsoft Entra, Sentinel, Defender for Cloud, and Purview. This incident, spanning from September 2 to September 19, 2024, has raised concerns about the company's ability to monitor and investigate security threats effectively. The lost logs are crucial for detecting breaches and malicious activities, and their absence could hinder organizations' efforts to identify and respond to potential security incidents during that period. This event has intensified scrutiny of Microsoft's security practices, especially following previous breaches linked to Chinese and Russian hackers.

Silent Threat: Red Team Tool EDRSilencer Disrupting Endpoint Security Solutions

Trend Micro's Threat Hunting Team has identified that threat actors are repurposing EDRSilencer, a red team tool originally designed to test security defenses, to disable endpoint detection and response (EDR) systems. By leveraging the Windows Filtering Platform, EDRSilencer blocks network communications of EDR processes, preventing them from sending telemetry or alerts to management consoles. This tactic allows malicious activities to evade detection, increasing the risk of successful ransomware attacks and operational disruptions. The misuse of such tools underscores the evolving threat landscape and the need for organizations to adopt proactive and adaptive security measures.

EU Adopts Cyber Resilience Act for Connected Devices

The European Union Council has officially adopted the Cyber Resilience Act (CRA), establishing EU-wide cybersecurity requirements for products with digital elements, including Internet of Things (IoT) devices. This regulation mandates that such products meet specific security standards throughout their lifecycle, encompassing design, development, production, and market availability. Products will bear the CE marking to indicate compliance, aiding consumers in identifying secure devices. Certain devices already governed by existing EU laws, like medical devices and aeronautical products, may be exempt. Following its publication in the EU's official journal, the CRA will enter into force 20 days later, with full application set for 36 months thereafter, though some provisions may apply earlier.

Ransomware Gangs Use LockBit's Fame to Intimidate Victims in Latest Attacks

Recent ransomware attacks have exploited Amazon's S3 Transfer Acceleration feature to exfiltrate victim data to attacker-controlled S3 buckets. The malware falsely claims to be LockBit ransomware, leveraging LockBit's notoriety to pressure victims into compliance. It embeds hard-coded AWS credentials, indicating a trend of attackers utilizing popular cloud services for malicious activities. Upon execution, the ransomware encrypts files and appends a unique extension, subsequently altering the device's wallpaper to display a LockBit 2.0 reference. This tactic underscores the evolving strategies of threat actors in the ransomware landscape.

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.

24/10/2024 – Zero-day vulnerability affecting FortiManager

Our Views:

Cybersecurity Training for the Workforce

Cybersecurity is a critical concern for New Zealand organisations due to the ever-increasing degree of business interruption, cost, and serious harm posed by successful cyber-attacks and data breaches. According to the latest Verizon Data Breach Investigations Report, 68% of all breaches are linked to attacks involving human error, highlighting the crucial role that employees play in securing company systems and information.

Malicious actors are continually targeting human vulnerabilities as they often find it easier to manipulate a user into compromising security, such as clicking a malicious link or mishandling data, rather than exploiting a technical vulnerability. Employees may unintentionally cause incidents through weak passwords, data mishandling, or the use of public-site passwords. A robust security program must therefore address these human vulnerabilities, considering varied risks across roles like executives or IT administrators.

The Center for Internet Security (CIS) uses data from the Verizon Data Breach Investigations Report to shape the CIS controls and best practices for workforce training. These controls emphasise employee education and awareness as essential layers of defence against cyber threats. For example, CIS Control 14, which addresses security awareness and skills training, integrates real-world data breach statistics to ensure that training programs cover the most pressing vulnerabilities and attack vectors.

Core Cybersecurity Training Requirements

Ensuring that all staff members understand cybersecurity policies and procedures is fundamental to a strong security posture. However, effective training programs not only focus on theoretical knowledge but also emphasise practical applications tailored to real-world scenarios.

The first step (14.1) in achieving an effective cybersecurity programme is to 'Establish and Maintain a Security Awareness Program'. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Organisations should conduct training at hire and, at a minimum, annually. Organisations should then review and update the content annually, or when significant enterprise changes occur.

Based on real world attack patterns, CIS suggests organisations structure their staff training and awareness initiatives to include the following:

CIS 14.2 to 14.8 Key Training Components

- **14.2 Recognizing Social Engineering Attacks:** Train workforce members to identify and avoid social engineering threats like phishing, business email compromise (BEC), pretexting, and tailgating.
- **14.3 Authentication Best Practices:** Educate employees on secure authentication practices, covering topics like multi-factor authentication (MFA), secure password creation, and effective credential management.
- **14.4 Data Handling Best Practices:** Instruct employees on properly storing, transferring, archiving, and destroying sensitive data. Include clear screen and desk policies, like locking screens when away, erasing whiteboards, and securing data assets.
- **14.5 Causes of Unintentional Data Exposure:** Make employees aware of common causes of unintentional data leaks, such as misdirected data, lost devices, or publishing to the wrong audience.
- **14.6 Recognizing and Reporting Security Incidents:** Train employees to identify and report potential security incidents promptly.
- **14.7 Identifying and Reporting Missing Security Updates:** Teach employees to check for missing patches or software updates and report any issues with automated security processes.
- **14.8 Dangers of Insecure Networks:** Educate employees on the risks of using insecure networks, including remote work guidance on securing home network configurations for safe data transmission.

Implementing an effective cybersecurity training program

Establishing and maintaining a security awareness program is essential to ensure that employees are security conscious and skilled in reducing cybersecurity risks to the enterprise. An impactful program should include frequent, relevant messages about security best practices tied to real-world events, such as password breaches or seasonal phishing scams.

To support New Zealand organisations in lifting overall workforce cybersecurity knowledge we have developed a learning management system (LMS) that provides training in all key cybersecurity knowledge areas outlined in the CIS controls.

We recommend organisations kick off their cybersecurity training programme with an instructor-led session. This session can lay a solid foundation for future online learning by explaining the importance of cybersecurity and the high stakes involved, backed by real-world examples and data such as the Verizon breach statistics.

This introductory session should then be followed with the LMS series of online courses designed for flexibility and engagement. The training content is divided into seven short, impactful four-minute videos that cover different aspects of cybersecurity, such as threat identification, data protection practices, and reporting mechanisms. After each video, a five-question quiz is included to reinforce learning and ensure comprehension.

To motivate employees and track progress, we provide a certificate of completion for those who successfully finish the course. Keeping a company record of these certificates can help your organisation maintain compliance and recognise employees' commitment to keeping the organisation secure.

By structuring training this way, companies can effectively communicate the significance of cybersecurity, create a culture of security awareness, and empower employees to be the first line of defence against cyber threats.

Visit cyber.thinkific.com to learn more about the LMS, sample some of the training, and if you wish to proceed, sign up to start your training program.

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: