NZ Incident Response Bulletin

Standard Edition – August 2024 – Issue #67

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

New Zealand completes cyber security review after IPAC threats

New Zealand has completed a cyber security review following threats from the Indo-Pacific (IPAC) region. The review identified critical areas where the country needs to strengthen its defences against cyber threats, emphasising the importance of collaboration between government, businesses, and international partners. The findings are part of New Zealand's broader strategy to address growing cyber risks and ensure the protection of national infrastructure and sensitive data.

Warehouse Group staffer hacks system, steals $95k vouchers to 'mess with bosses'

A 25-year-old employee from The Warehouse Group in Hamilton, hacked into the company's system to steal $95,000 worth of vouchers as revenge for what he perceived as unfair treatment. He used his access to manipulate spreadsheets and redeem the vouchers, purchasing expensive items. Some stolen goods were recovered, but much was sold to second-hand stores. He was sentenced to 10 months' home detention and ordered to repay $10,000 at $100 per week, though full repayment is unlikely.

CrowdStrike glitch: Kiwi firms warned to stay vigilant as hack threats linger

A recent glitch in CrowdStrike's cybersecurity software affected 8.5 million Windows devices globally, disrupting flights, retail, banking, and healthcare systems. While the issue has been largely resolved, New Zealand companies are warned to stay vigilant as scammers may exploit the situation. Cybersecurity experts stress the importance of updating software with the latest patches and being cautious of phishing attempts impersonating CrowdStrike or Microsoft.

Australia

Major Australian bank raises alarm bell on cyber 'warfare': Claims 'entire community is at risk'

Westpac, a major Australian bank, has raised significant concerns about the rising threat of cyber warfare, emphasising that it poses a risk to the entire community, not just individual entities. The bank's CEO, Peter King, highlighted that the sophistication and frequency of cyberattacks are escalating, potentially causing widespread financial and operational disruptions across various sectors. Westpac is advocating for a united front, urging both public and private sectors to bolster their cybersecurity measures and collaborate more closely to counter these growing threats effectively.

Australia to pilot 'long overdue' cyber threat-sharing network for healthcare

Australia is launching a pilot program for a cyber threat-sharing network in the healthcare sector. This initiative aims to improve cybersecurity by enabling healthcare organisations to share information about cyber threats and vulnerabilities in real-time. The network is considered long overdue given the increasing frequency of cyberattacks targeting the healthcare industry. It will help healthcare providers better protect patient data and maintain the integrity of their systems.

Australian government mandates cybersecurity framework, stresses global OT/ICS collaboration

The Australian government has mandated a new cybersecurity framework, emphasising the need for collaboration between global Operational Technology (OT) and Industrial Control Systems (ICS) sectors. This move is part of Australia's broader strategy to enhance cybersecurity across critical infrastructure. The framework aims to improve resilience against cyber threats and promote international cooperation to address shared challenges in protecting vital systems and networks.

World

Threat actor impersonates Google via fake ad for Authenticator

A recent threat has emerged where a cybercriminal impersonates Google through a fake ad promoting a malicious version of Google Authenticator. The ad lures users to a phishing site that appears legitimate, but instead of downloading the actual app, it installs malware. This malware can steal sensitive information, including authentication codes. The attack highlights the importance of downloading apps only from official sources to avoid such scams.

Microsoft confirms Azure, 365 outage linked to DDoS attack

Microsoft's Azure and Microsoft 365 services experienced significant outages due to a Distributed Denial of Service (DDoS) attack. The attack disrupted services for many users, highlighting vulnerabilities in cloud infrastructure. Microsoft has since mitigated the attack and restored services, but the incident underscores the growing threat of cyberattacks targeting major service providers. Microsoft is working to strengthen its defences against future incidents and ensure the reliability of its cloud services.

UK Cyber Bill teases mandatory ransomware reporting

The UK's upcoming Cyber Security Bill may introduce mandatory ransomware reporting requirements for businesses. This move aims to improve national cybersecurity by ensuring that incidents are reported promptly, allowing for quicker response and mitigation. The bill could also include measures to enhance information sharing between organisations and government agencies, which would help in tackling cyber threats more effectively. The legislation is part of the UK's broader efforts to strengthen its defences against the growing threat of cyberattacks.

10 Major Cyberattacks And Data Breaches In 2024 (So Far)

The article highlights ten major cyberattacks and data breaches that occurred in 2024, affecting various sectors globally. These incidents include ransomware attacks, data leaks, and breaches that exposed sensitive information, leading to significant financial and reputational damage. The article emphasises the growing sophistication of cybercriminals and the increasing frequency of such attacks, underscoring the urgent need for enhanced cybersecurity measures across organisations to mitigate these risks.

Scattered Spider Adopts RansomHub and Qilin Ransomware for Cyber Attacks

The article discusses how the cybercriminal group Scattered Spider has adopted a new tactic called "RansomHub," a centralised platform for managing and deploying ransomware attacks. This development marks a significant evolution in the group's operations, enabling them to target organisations more efficiently and scale their attacks. The use of RansomHub demonstrates the increasing sophistication of cybercriminals and highlights the growing threat posed by such coordinated ransomware campaigns.

LA County Superior Court hit by ransomware attack

The Los Angeles County Superior Court experienced a significant ransomware attack that disrupted its operations, leading to the shutdown of several systems as a precautionary measure. The attack is under investigation, with efforts focused on determining the extent of the data breach and restoring services. This incident underscores the vulnerability of public institutions to cyberattacks and highlights the ongoing threat they pose to critical infrastructure and services. The court is working diligently to recover and ensure the security of its systems moving forward.

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.

19/07/2024 - Widespread IT Outage Due to CrowdStrike Update

Our Views:

The Importance of Business Continuity and Disaster Recovery Planning

As evidenced by the recent widespread CrowdStrike issue, organisations face a myriad of risks that can disrupt operations. From natural disasters to cyberattacks, these unforeseen events can have severe consequences on a business's continuity and financial stability. This is where Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) become indispensable. These plans are not just essential for, but also for maintaining operations during and after a disaster.

Understanding BCPs, DRPs and IRPs

While BCPs, DRPs and IRPs are often used interchangeably, they serve different purposes as follows:

- Business Continuity Plans (BCPs): These plans are proactive, focusing on maintaining normal operations before, during, and immediately after a disaster. They ensure that business functions continue with minimal interruption, thus mitigating financial and operational impacts.
- Disaster Recovery Plans (DRPs): In contrast, DRPs are reactive, detailing the steps necessary to respond to an incident and restore operations smoothly. They concentrate on IT systems and data, crucial for protecting vital information and reducing downtime during crises.
- Incident Response Plans (IRPs): An IRP is designed to manage and mitigate the effects of security incidents. It outlines procedures for detecting, responding to, and recovering from security breaches, focusing on minimising damage and restoring normal operations.

While BCPs, DRPs, and IRPs are all critical, their distinct focus areas necessitate separate development. While we usually spend a lot of time discussing IR Planning, the focus below will be on BCPs and DRPs.

The Benefits of Effective Business Continuity and Disaster Recovery Planning

Effective Business Continuity and Disaster Recovery planning may enable:

- Shortened Downtime: Effective BCPs and DRPs help organisations minimise downtime and quickly restore operations, reducing the financial impact of disruptions.
- Lower Financial Risk: Strong BCPs can significantly reduce disruption costs by maintaining customer confidence and ensuring quick recovery.
- Protection Against Reputational Damage: A well-executed BCP and DRP protect an organisation's reputation by demonstrating preparedness and the ability to handle crises efficiently.
- Reduced Penalties: Robust BCPs ensure compliance with regulatory requirements, mitigating the risk of substantial penalties due to data breaches or other incidents.

The Regulatory Perspective

Regulative requirements, such as those outlined in the "Regulatory Impact Statement: Business Continuity Condition for FMC Licences," now underscore the importance of BCPs and DRPs. Effective July 1, 2024, this new standard condition mandates certain market services licence holders under the Financial Markets Conduct Act 2013 (FMC Act) to maintain robust business continuity plans and critical technology systems.

Objectives of the Regulation include:

- Ensuring licence holders maintain business continuity plans and operational resilience of their critical technology systems.
- Providing timely information to the Financial Markets Authority (FMA) about incidents impacting these systems.

This regulation highlights the necessity for organisations to have solid plans to not only safeguard their operations, but also to comply with legal and regulatory standards, thus avoiding penalties and maintaining their reputation.

Building Effective BCPs and DRPs

Before diving into the specifics of creating effective BCPs and DRPs, it's essential to understand two key concepts: Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

- Recovery Time Objective (RTO): This refers to the maximum acceptable amount of time it takes to restore business processes after an unplanned incident. Establishing a reasonable RTO is a critical first step in both BCP and DRP development. The goal is to minimise downtime and ensure that operations can resume as quickly as possible.
- Recovery Point Objective (RPO): RPO is the maximum acceptable amount of data loss measured in time. It reflects the point in time to which data must be restored to resume operations after a disaster. Businesses often have different RPOs depending on their data protection strategies. Some enterprises continuously copy data to a remote data centre to ensure no data loss, while others may tolerate a few minutes or hours of data loss, knowing they can recover from a backup system.

Once you understand your RTO and RPO the following high-level steps are actioned to create BCP and DR plans:

1. Conduct a Business Impact Analysis (BIA): Identify critical business functions and processes and assess the potential impact of various types of disruptions. This analysis helps prioritise which areas need immediate attention and resources.
2. Identify Risks and Threats: Determine the potential risks and threats that could impact your business. This could include natural disasters, cyber-attacks, equipment failures, or other emergencies. Understanding these risks helps in developing targeted strategies for both continuity and recovery.
3. Inventory Your Assets: Conduct regular inventories of all IT assets, categorising them as critical, important, or unimportant to prioritise protection and recovery efforts.
4. Develop Recovery Strategies: Based on the BIA and risk assessment, create strategies to maintain and restore critical functions. For BCPs, this might involve setting up alternate work sites or remote working capabilities. For DRPs, it could include specific procedures for data recovery, system repairs, and communication plans.
5. Establish Roles and Responsibilities: Clearly define who is responsible for various tasks during a disaster. This includes identifying key personnel, their roles, and the chain of command. Having a clear structure ensures that everyone knows their duties and can act quickly.
6. Create Communication Plans: Effective communication is vital during a disaster. Develop plans for internal and external communications to ensure that employees, stakeholders, and customers are informed and updated regularly.
7. Implement Training and Testing: Regular training sessions and drills help ensure that all team members are familiar with the BCP and DRP procedures. Conducting tests and simulations can identify any weaknesses in the plans and provide opportunities for improvement.
8. Review and Update Plans Regularly: BCDR plans should not be static. Regular reviews and updates are necessary to accommodate changes in business processes, technology, and emerging threats. Continuous improvement helps keep the plans relevant and effective.

The integration of Business Continuity Plans and Disaster Recovery Plans is crucial for organisational resilience. These plans not only help businesses prepare for and respond to unexpected incidents but also ensure compliance with regulatory requirements, thus safeguarding financial stability and reputation. By understanding the differences between BCPs, DRPs, and Incident Response Plans (IRPs) and following the steps to create and maintain these plans, organisations can enhance their ability to withstand and recover from disruptions, ensuring long-term sustainability and success. The new standard condition introduced by the FMA serves as a key example of the regulatory emphasis on the importance of these plans, further highlighting their critical role in today's business environment.

NZ Incident Response Bulletin

Standard Edition – August 2024 – Issue #67

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: