# NZ Incident Response Bulletin

## Standard Edition – July 2023 – Issue #54

*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

Customer refunded $60k lost to 'IR' phishing scam

There's a warning from the Banking Ombudsman that online phishing scams are becoming increasingly sophisticated. It recently ruled that a customer should be reimbursed the full $60,000 he lost when he responded to an email he thought was from Inland Revenue. He entered his banking details and an SMS code into a fake website because he thought he was dealing with IR and his bank but ended up losing the money.

"Ordinarily, banks are liable for a customer's losses as a result of an unauthorised transaction - typically a scam - if the customer has taken reasonable care to protect his or her banking. In this case, such was the sophistication of the scam that we considered the customer had shown reasonable care in the circumstances," Banking Ombudsman Nicola Sladden said.

Auckland City Police make multiple arrests after millions lost through online scams

The Auckland City Financial Crime Unit are making arrests as investigations continue into reports of a scam type involving term deposits, duping victims out of millions of dollars. This month a third significant arrest has been made for Money Laundering. It comes after warnings to the public of the emerging sophisticated scam making the rounds, which involves a victim searching term deposits online. The victim finds a bank they want to go with and provide their contact details on a 'bank' website, which is in fact a fake website run by a scammer. The 'bank' then calls the victim to open a new term deposit, the victim transfers money into a New Zealand-based account held by a money mule who then sends the funds offshore.

Regulator satisfied with NZX technology posture after 2020 DDoS attack

The Financial Markets Authority has completed a review of the NZX's technology capabilities and found it has complied with its obligations. After the share market operator suffered a highly disruptive denial of service attack in 2020 the regulator found it had failed to meet its licensed market operator obligations due to insufficient technology resources. The attack was described as "foreseeable" while the NZX's crisis management planning and procedures were described as "basic". The market regulator undertook a review of the NZX's technology capabilities across its people, processes and platforms and the NZX subsequently developed and worked through an action plan to address the findings of that review.

More vigilance urged as cyber crime losses soar by two-thirds in value

Financial losses from cyber crimes rose 66 percent in the first three months of the year over the previous quarter, amounting to nearly $6 million in losses. CERT NZ (Computer Emergency Response Team) said scammers were using a number of new tactics to rob people of investments, as well as scams involving romance and an increasing use of artificial intelligence (AI). It said the number of scams was trending higher, with a 23 percent increase from the last three months of 2022 (Q4 2022), as criminals used search engine ads and professional-looking documentation to scam New Zealanders looking to invest money. A scam campaign in February cost New Zealanders millions of dollars in a very short time, which demonstrated how quickly someone could lose their assets.

## World

SEC Alleges SolarWinds CFO, CISO Violated US Securities Laws

The Securities and Exchange Commission (SEC) accused SolarWinds CFO Bart Kalsu and CISO Tim Brown of violating securities laws in their response to a high-profile software supply chain cyberattack in 2020. The Austin, Texas-based IT infrastructure management vendor revealed that Kalsu and Brown are among "certain current and former executive officers and employees" targeted by the SEC for their role in responding to the Russian hack of the Orion network monitoring product. For each individual, SEC staff have recommended filing a civil enforcement action alleging violations of federal securities laws.

APRA hits Medibank with $250m punishment for breach

Medibank Private will have to set aside $250 million as insurance against issues associated with a major data breach last year, with the prudential regulator also reviewing the company's "governance and risk culture". The decision by the Australian Prudential Regulation Authority would likely "increase the risk of adverse class action rulings" against the company, according to equities analysts at JPMorgan.

The additional capital adequacy requirement, which came as a surprise to some in the market, was "a short to medium term negative for the stock itself, and arguably indicates increased risk of adverse findings in the class actions against them relating to the cyber breach", the investment bank wrote in a note to clients.

Australia's Privacy Watchdog Hacked by Russians

The government agency tasked with monitoring privacy breaches from cyber attacks has itself been hacked – and failed to notify Australians who may have had their information compromised. The Office of the Australian Information Commissioner has had data stolen by the Russian criminal ransomware gang known as BlackCat, or ALPHV. The data was stolen through legal firm HWL Ebsworth, who the OAIC is a client – according to a report by The Australian.

NDIS agency scrambles over risk of leaked sensitive client information in HWL Ebsworth hack

The agency responsible for the national disability insurance scheme is scrambling to learn whether sensitive client information related to appeal cases has been caught up in a large cybersecurity hack on the law firm HWL Ebsworth which has represented the agency.

The Russian-linked ALPHV/Blackcat ransomware group said in a post on the dark web in late April that data from the law firm had been hacked. Earlier this month, the group published some of the data it claimed to have stolen – later established to be 3.6TB worth of data, of which 1.1TB has been posted.

Clop ransomware gang starts extorting MOVEit data-theft victims

The Clop ransomware gang has started extorting companies impacted by the MOVEit data theft attacks, first listing the company's names on a data leak site—an often-employed tactic before public disclosure of stolen information. These entries come after the threat actors exploited a zero-day vulnerability in the MOVEit Transfer secure file transfer platform on May 27th to steal files stored on the server. The Clop gang took responsibility for the attacks, claiming to have breached "hundreds of companies" and warning that their names would be added to a data leak site on June 14th if negotiations did not occur.

Microsoft says hacktivist group Anonymous Sudan was behind Office outage this month

Microsoft has confirmed hackers were responsible for a serious outage of Office suite programs this month. The Outlook email, OneDrive and cloud computing platform were all plagued by sporadic disruptions, for which a shadowy hacktivist group claimed responsibility. Initially, Microsoft was reticent to confirm the attack, but the company now says a group called Anonymous Sudan is behind the outage. The group claimed responsibility on its Telegram social media channel at the time. Some security researchers believe they're Russian.

## 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.

6/06/2023 – Securing Remote Access Software

12/06/2023 – Fortinet Releases Security Updates for FortiOS and FortiProxy

14/06/2023 – Understanding Ransomware Threat Actors: LockBit

## Our Views:

### Key Takeaways from the 2023 Data Breach Investigation Report

The annual Verizon Data Breach Investigation Report gives us one of the most reliable and comprehensive insights into the recent cyber incident and data breach landscape. It describes the main challenges and threats organisations have faced over the previous 12 months. It is also a key resource that The Centre for Internet Security uses to continually help them recommend the most relevant and effective security controls an organisation can implement to combat these threats.

The 2023 report analyses a total of 16,312 security incidents whereby a security event compromised the integrity, confidentiality, or availability of information assets. 5,199 of these incidents were confirmed data breaches. We have included the highlights and what we consider the key learnings from this latest report below:

**Threat Actors**

- External actors were responsible for most confirmed data breaches (83%). These external actors were overwhelmingly (94.6%) financially motivated with organised crime groups making up around three quarters of these actors.
- Nation state sponsored data breaches were not highly represented with internal end users contributing to more data breaches via either malicious activity or accident than state affiliated actors.

**Attacks, Attack Vectors, and Assets**

- The Use of Stolen Credentials followed closely by Ransomware and then Phishing rank as the most used attack actions when reviewing all confirmed data breaches.
- Denial of Service attacks and Ransomware dominate the statistics when looking at all incidents.
- The top three attack vectors for both confirmed data breaches and incidents in order of prevalence were:
  - Web application
  - Email
  - Carelessness
- Ransomware was involved in almost a quarter of all breaches and still appears to have room to grow further and cause greater harm in the years to come. The latest data suggests that while ransom demand amounts have lowered the overall cost to recover from a ransomware attack is increasing.
- Social Engineering attacks have increased. Business Email Compromise has almost doubled since the previous year with pretexting and phishing the primary attack actions. 50% of all Social Engineering incidents in 2022 used pretexting. Pretexting is essentially an invented scenario that tricks someone into handing over information or doing something that may result in a breach.
- Poor creation and protection of passwords drove high rates of Basic Web Application attacks this year. Leveraging stolen credentials and vulnerabilities enabled 25% of data breaches.
- The top attack patterns of System Intrusion, Basic Web Application Attacks, and Social Engineering ensured Servers remained the top asset affected by a breach, particularly Web Application and Email Servers. People take the second spot reflecting the impact of social engineering.
- Operational Technology impacts still feature extremely low in comparison to impacts on Information Technology making it hard to derive valuable information on this area yet.
- Denial of Service attacks dominate the overall incident category where median bits per second in these attacks grew by 57% from 1.4 Gigabytes per second previously to 2.2Gbps this year.

**Important actions to take in response to this information include:**

- New remote and more flexible working models mean devices and data are more likely to be transported and used in multiple locations. This requires business to monitor and act to prevent carelessness and loss. Remind employees about their duty of care and set guidelines for the storage and protection of assets.
- Ransomware response plans should be in place and understood by all in the organisation.
- Employee awareness training to address good credential management, general landscape awareness, and phishing identification remains critical to combat social engineering (CIS 14 as below).
- Review your DDOS mitigation service to ensure it can scale appropriately and ensure DNS infrastructure resiliency.
- Consider implementing or augmenting a Software Bill of Materials (SBOM) process where relevant.
- The following set of critical security controls should be considered as priority actions for your business:
  - CIS 4 Secure Configuration of Enterprise Assets and Software (4.1, 4.2, 4.4, 4.5)
  - CIS 5 Account Management (5.1, 5.3)
  - CIS 6 Access Control Management (6.1, 6.3, 6.4) MFA,MFA,MFA!
  - CIS 7 Continuous Vulnerability Management (7.1,7.2)
  - CIS 9 Email and Web Browser Protection (9.2)
  - CIS 10 Malware Defences (10.1, 10.2)
  - CIS 11 Data Recovery (including 11.1, 11.2, 11.3, 11.4)
  - CIS 14 Security Training and Awareness
  - CIS 17 Incident Response Management (17.1,17.2,17.3)

**Regional Differences**

Overall, the APAC (Asia Pacific) region generally follows similar patterns to all other regions with a couple of notable differences. Social Engineering rates as the highest problem in the APAC region with System Intrusion second. This contrasts with all other regions where System Intrusion dominates. Additionally, the percentage of espionage attacks and the resulting compromise of data secrets is significantly greater in APAC than other regions.

In summary the DBIR highlights some key areas of concern for organisations. As a priority we recommend you invest in your people. Security awareness training is crucial as 74% of breaches involved the human element. You should back up this awareness training with smart policies, processes and automated systems that aid in compliance. Secondly, as threats continue to accelerate you should assess your organisation against each of the CIS controls outlined above and take steps towards closing any gaps.

Further detail on all the report detail including mapping to the Mitre Attack framework is available on the Verizon website.

## 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: