NZ Incident Response Bulletin

Standard Edition - August 2019

In this issue:

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

Cyber-resilience in FMA-regulated financial services

On 11 July 2019, the Financial Markets Authority (FMA) released a report on their review of cyber-resilience in New Zealand financial services. The report summarises the findings and provides guidance for firms where the need for improvement has been identified. The FMA has encouraged sector participants to comply with its expectations and best practice.

"Cyber-risk encompasses all risk of loss, disruption, or damage to a firm caused by failure in its information technology systems – from both internal and external threats. The interconnectedness of the financial sector means any part of it might be an entry point for a wider cyber-incident."

The report goes on to recommend that all market participants should assess cyber-risk as part of their wider risk-assessment and management programme. "We also strongly encourage all market participants to use a recognised cybersecurity framework" and recommends "The National Institute of Standards and Technology (NIST) cybersecurity framework core, for example, enables firms to assess maturity across five functions: Identify, Protect, Detect, Respond, and Recover."

Note that we have moved to larger premises.
Our new address and phone number is:
Plaza Level, 41 Shortland St, Auckland 1010
0800 WITNESS (0800 948 637) or 021 779 310

NZ Incident Response Bulletin

Standard Edition - August 2019

[Awareness of whistle-blowing legislation alarmingly low]

Over the last month there has been an increase in the number of public reports regarding Whistleblowers in New Zealand. The Office of the Ombudsman recently published a media release detailing the results of research it had undertaken. According to the Ombudsman, public awareness of the Protected Disclosures Act (PDA) is very low. Key findings include:

- Only 9% of respondents said they were aware of the PDA
- 21% of all respondents said they have witnessed serious wrongdoing at their workplace or previous workplaces
- 40% of all respondents, currently in work, felt their jobs would be safe if they reported the wrongdoing, 34% said their job wouldn't be safe and 27% were unsure
- Respondents who knew about the PDA were more likely to feel their job would be safe if they reported wrongdoing (62%).

According to the Ombudsman, "there is a clear difference here between those who know about the Act and those who don't, and that's concerning". "Everyone reporting serious wrongdoing should have total faith that they are protected under the Act. The fact that so many people seem unaware suggests this important law is not working as well as it should".

World

[Capital One Data Breach Compromises Data of Over 100 Million]

A software engineer in Seattle hacked into a server holding customer information for Capital One and obtained the personal data of over 100 million people in one of the largest thefts of data from a bank.

The suspect, Paige Thompson, 33, left a trail online for investigators to follow as she boasted about the hacking, according to court documents in Seattle. She was arrested and charged with one count of computer fraud and abuse.

The F.B.I. agent who investigated the breach said in court papers that Ms Thompson had gained access to the sensitive data through a "misconfiguration" of a firewall on a web application. This allowed the hacker to communicate with the server where Capital One was storing its information and, eventually, obtain customer files.

According to the criminal complaint, a tipster wrote to a Capital One security hotline, warning that some of the bank's data appeared to have been "leaked."

Capitol One said in a news release that it had "immediately fixed the configuration vulnerability" once it discovered the problem.

[Baltimore City Council committee approves $10 million in funding for ransomware recovery]

The Baltimore City Council approved a $10 million payment to cover the costs to recover from a ransomware attack that brought down city computer networks, with a further $8 million being accounted for in lost revenue.

Hackers broke into the city's networks, locked files and demanded a ransom equivalent to $76,000 to turn over the digital keys, however the city refused to pay. So far, city officials have disclosed that they have spent $2.8 million hiring security consultants and other companies; $486,000 on technicians to set up new computers; $112,000 on overtime for city staff, and $1.9 million on new hardware and software.

When the city's IT leaders were asked whether they had a written disaster response plan before the attack, they acknowledged they did not. Officials said it could take nine months to produce a plan.

On 30 July 2019, a joint group of US Government Agencies including The Cybersecurity and Infrastructure Security Agency released a Joint Ransomware Statement with recommendations for state and local governments to build resilience against ransomware. One recommendation is to ensure response plans include how to request assistance from external cyber first responders in the event of an attack.

NZ Incident Response Bulletin

Standard Edition - August 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "Improving Cyber Resiliency using NIST and the Cybersecurity Framework".

On 11 July 2019, the Financial Markets Authority (FMA) released a report on cyber-resilience in New Zealand financial services. The report recommends The National Institute of Standards and Technology (NIST) Cybersecurity Framework as an example to assist with planning, prioritising and managing cyber-resilience. We explore this framework and suggest several practical steps you can take.

Automating the NIST Cybersecurity Programme

The NIST Cybersecurity Framework can be used to either develop or improve upon a cybersecurity programme. Given there are 108 sub-categories which define the framework, we recommend where possible, automating your programme. The main phases include assessments of your current profile and target profile, and based on the variances, establishing a roadmap of improvement actions.

Your conformance with the programme and priority areas can then be re-assessed as often as you like without the need to re-produce time intensive reports. At a high level, your programme should include at least the following outputs:

- A heat map of your assessment scores;
- A variance between your current and target profiles; and
- A list of informative references to make improvements to your current profile.

Respond and Recover Key Considerations

Much attention is paid to the three functions of "Identify", "Protect" and "Detect". But what if you suffer a cyber-attack? How prepared are you to "Respond" and "Recover"? These are the two functions that Incident Response and Forensic Technology specialists most commonly deal with. Regardless of your organisations cyber-security profile maturity, we recommend ensuring you have at least considered the following NIST recommendations:

- Execute and maintain processes and procedures when responding to detected cybersecurity incidents and when recovering systems or assets affected by cybersecurity incidents.
- Coordinate response activities with internal and external stakeholders.
- Personnel should know their roles and order of operations when a response is required.
- Conduct analysis to ensure an effective response and to support recovery activities. Perform forensics where required.
- Fully understand the impact of the incident.
- Perform activities to prevent the expansion of the incident.
- Mitigate newly identified vulnerabilities or document as accepted risks.
- Improve response and recovery planning by incorporating lessons learned into future activities.

NIST Resources to Improve Forensic Preparedness

The NIST website provides numerous resources to assist with forensic procedures in the event of a cybersecurity incident. Examples include:

- The 'National Software Reference Library', which consists of an exhaustive collection of known files that can be eliminated from any examination.
- 'Computer Forensics Tool Testing' consists of general tool specifications, test procedures, test criteria, test sets and test hardware.
- 'Computer Forensic Reference Data Sets' consists of documented sets of simulated digital evidence for examination.

NZ Incident Response Bulletin

Standard Edition - August 2019

Upcoming Events:

Date	Event	Location
2 September 2019	CAANZ Fraud & Forensic Conference 2019	Auckland
11-13 September 2019	ISACA 2019 Oceania CACS Conference	Auckland
16, 18, 20 September 2019	SSS Cyber Security Day 2019	Christchurch, Auckland, Wellington
16 October 2019	2019 NZ Cyber Security Summit	Wellington

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.

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

Share our Bulletin: