NZ Incident Response Bulletin

Standard Edition - July 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

New Zealand's Cyber Security Strategy 2019

Minister of Broadcasting, Communications and Digital Media, Hon Kris Faafoi, released the latest Cyber Security Strategy on 2 July 2019.

Cyber-enabled threats to New Zealand's security continue to grow in number, scope and scale. The Cyber Security Strategy 2019 outlines the areas where Government will prioritise action and how it will work together with individuals, businesses, and communities to ensure that New Zealand is confident and secure in the digital world.

The refreshed strategy has five priority areas that build on the previous strategy, while reflecting current cyber security challenges:

- Cyber security aware and active citizens
- Strong and capable cyber security workforce and ecosystem
- Internationally active
- Resilient and responsive New Zealand
- Proactively tackle cybercrime.

Note our new phone number:

0800 WITNESS

NZ Incident Response Bulletin

Standard Edition - July 2019

N4L completes ICT upgrade for schools across NZ

Crown company Network for Learning (N4L) says schools across New Zealand are now better protected from cyber threats and harmful websites following the nationwide rollout of new technology. The rollout covers 825,000-plus students, teachers and school staff across New Zealand with smart and safe internet for teaching and learning. According to N4L, the new system has already prevented millions of malicious online threats and inappropriate websites from reaching New Zealand schools and their students.

World

Cyber-attack hits police forensic work

Eurofins Forensic Services carries out DNA testing, toxicology analysis, firearms testing and computer forensics for police forces across the UK. Its parent company, Eurofins, suffered a ransomware attack on 1 or 2 June.

The National Police Chiefs' Council (NPCC) took the decision to "temporarily suspend" all submissions to Eurofins, leading to delays in forensic testing, which could impact on court cases. NPCC lead for forensics, Chief Constable James Vaughan said "Our priority is to minimise the impact on the criminal justice system."

Eurofins said the attack "caused disruption to many of its IT systems in several countries" in a statement on its website. It said it believed the attack was carried out by "highly sophisticated well-resourced perpetrators" and the ransomware involved appears to have been a "new malware variant".

The National Crime Agency is investigating the cyber-attack, supported by the National Cyber Security Centre. A government spokesperson said: "We are working closely with law enforcement and justice partners to investigate the sources of the attack and minimise any impact on our criminal justice system."

While not related to the cyber-attack, it is also noteworthy that The England & Wales Forensic Science Regulator has recently established a Whistleblower platform for experts to call regarding aspects of forensic sampling and analysis that enter the Criminal Justice System.

Former Equifax exec gets 4 months in prison for insider trading after breach

A former Equifax executive, who sold his stock in the consumer credit reporting firm before it announced a massive data breach, has been sentenced to four months in federal prison for insider trading. Jun Ying, former chief information officer for the company's US Information Solutions, was also ordered to pay about $117,000 in restitution and a $55,000 fine.

In 2017, Equifax announced that it suffered a data breach that would affect more than half of the US population, exposing the Social Security numbers, names and addresses of 147 million Americans. The company learned about the breach on 29 July 2017, but didn't announce it publicly for nearly three months.

On 25 August 2017, Ying texted a co-worker about the breach, saying it "sounds bad. We may be the one breached," according to the indictment. The next week, Ying conducted a web search to learn what happened to Equifax's stock price after the company experienced a data breach in 2015.

Three days later, Ying sold all his shares in Equifax, making more than $950,000. Ying's insider trading happened 10 days before Equifax publicly announced its breach.

NZ Incident Response Bulletin

Standard Edition - July 2019

Our Views:

A selection of issues relevant to Forensic and Cyber Security matters during the last month. This month's theme is "NZ Cyber Security Strategy 2019".

The NZ Cyber Security Strategy 2019 was released on 2 July 2019. The New Zealand Government has set out five priority areas to improve cyber security (2019–2023). We explore several of these in detail and suggest several practical steps you can take.

Cyber security aware and active citizens

Building a culture in which people can operate securely online and know what to do if something goes wrong.

1. Understand cyber security in the context of your organisation and sector; and educate accordingly. If you handle payments, health information, intellectual property or are a nationally significant organisation, your risk is higher.
2. There are numerous fit for purpose cyber security awareness tools available to assist organisations build awareness and resilience. Conduct a search online and contact several providers to explore your needs.
3. Initiate a yearly employee cyber security 'Warrant of Fitness' check.
4. Have a trusted person or organisation on 0800 speed dial for when you need cyber incident response assistance. They will know how to respond and which Government agencies to contact.

Resilient and responsive New Zealand

Ensuring that New Zealand can resist cyber threats and that we have the tools and know-how to protect ourselves.

1. Adopt a suitable cyber programme such as the National Institute of Standards and Technology Cyber Security Framework (NIST CSF).
2. Recognise that New Zealand is not immune to the threat of cyber-attack and defend accordingly. Say to yourself, it can happen to us and we may already have been compromised. Undertake a breach assessment check.
3. Understand your cyber threat landscape by conducting research and share information amongst your employees, third parties and other key stakeholders. A monthly dashboard is a good starting point.
4. Be prepared to respond to major cyber incidents. Develop an operational cyber strategy, distribute an incident response plan and conduct regular cyber simulations.

Proactively tackle cyber-crime

Cyber-crime has existed in New Zealand for decades and the incidence of attacks continues to increase exponentially. The New Zealand Government has its role to play, but you will also need to be actively involved in preventing and responding to attacks, both from external and internal threat actors.

There is evidence that proves that the consequences of cyber-crime are becoming more severe. It may be that small actions can prevent the worst crimes, for example, turning on two factor authentication on any cloud service such as email, file drops and the like can prevent millions of dollars' worth of theft and fraud.

Cyber-criminals pivot, so should you. Consult with experts who can help you understand and tackle cybercrime; for example:

Year	Threat	Mitigation
2018	Ransomware	Anti-malware and Backups
2019	Business Email Compromise	Two factor authentication and Phishing awareness campaigns
Emerging	Remote Access Compromise	Uninstall any free remote access tools and replace with commercial grade ones, or better still eliminate remote access

NZ Incident Response Bulletin

Standard Edition - July 2019

Upcoming Events:

Date	Event	Location
19-20 August 2019	Gartner Security & Risk Management Summit 2019	Sydney, Australia
2 September 2019	CAANZ Fraud & Forensic Conference 2019	Auckland
11-13 September 2019	ISACA 2019 Oceania CACS Conference	Auckland
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

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.

Share our Bulletin: