# NZ Incident Response Bulletin

Standard Edition - March 2020

## In this issue:

| News | Our Views | Upcoming Events |
|---|---|---|
| New Zealand | Identity Crimes | Cyber Security: The Good, The Bad and the Ugly |
| World | | Future of Security |
| | | RSA Conference 2020<br>Asia Pacific & Japan |

*Refer to our Premium Edition for additional information on Threat Alerts, Security Frameworks, Information Security Surveys, Forensic News and Research.*

## 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

The Reserve Bank estimates cyber-attacks could have significant financial impact on economy

New Zealand's central bank said that cyber-attacks could wipe off about 2 to 3 percent of the profits of the banking and insurance industries each year, highlighting the need for the industry to counter these threats. Cyber-attacks could cost an average of NZ$104 million for the banking sector and NZ$38 million for the insurance sector annually. The estimate model also indicated that in any given year there is a 5 percent chance of costs exceeding NZ$2.3 billion a year. RBNZ said it was strengthening efforts to enhance the resilience of the financial system, including developing risk management guidance and promoting information-sharing in collaboration with industry and other public organisations.

Phil Goff's emails hacked - 15,000 emails over 12 years offered for sale

Auckland mayor Phil Goff suffered an alleged hack of his family email account with a seller offering more than 15,000 of his emails online at a $20,000 price tag. The stolen emails appear to include confidential data including polling data from the 2018 mayoral campaign, fundraising plans, and sensitive business information. Use of private and unsecured email systems for sensitive business is not recommended and ideally a barrier between private email and corporate systems should be in place to prevent data transfer. Phil Goff himself has been quoted saying "Anything (of) an official nature should be going through protected channels."

New Zealand condemns malicious cyber activity against Georgia

New Zealand has joined a number of other countries to condemn the October 2019 cyber-attack against Georgia by Russian state actors. Over 2,000 Georgian websites and the Georgian national television station were impacted by the attack. "New Zealand supports the call for an end to this type of irresponsible activity. These malicious cyber activities serve no legitimate interest." - Andrew Hampton, Director-General of the Government Communications Security Bureau (GCSB). The GCSB hope that by recognising the attribution of these attacks to Russian state actors they can deter such state led activity in the future.

**Read our latest publication "Cyber Security Guide for NZ Law Firms"**

# NZ Incident Response Bulletin

Standard Edition - March 2020

## World

### Australian man allegedly stole more than 80 people's identities to pocket NZ$11.5m

An Australian man has been charged over a NZ$11.5 million cyber fraud. It is estimated the man gained more that NZ$11.5 million through identity theft and the establishment of fraudulent accounts.

Police allege the man obtained the personal details of several unrelated individuals across Australia – such as their date of birth, credit card numbers and bank account details – and used these details to modify payroll data, superannuation details and credit card records. In one unsuccessful example he allegedly tried to transfer more than NZ$1.15 million from one victim’s superannuation account to his own. The bank however flagged and stopped this transaction.

Police are yet to determine how Jones allegedly obtained the victims' identities, however various electronic equipment was seized and is undergoing forensic examination.

"Cybercrime presents a unique challenge for law enforcement. Identity information is a valuable commodity on the black market and dark web, and anyone who stores this data needs to ensure it is protected," - NSW Cybercrime Squad Commander Detective Superintendent Matthew Craft.

Recent figures from the Attorney-General's Department estimate that identity crime costs Australia upwards of A$1.6 billion each year.

### Hackers Were Inside Citrix for Five Months

Citrix systems has announced recently that malicious hackers were inside its networks for five months in 2018 and 2019. The hackers took personal and financial data on employees, contractors, interns and job candidates from their systems before they were discovered. The data taken may have included Social Security Numbers, tax identification numbers, driver’s license numbers, passport numbers, financial account numbers, payment card numbers and limited health claims information.

In March 2019 the FBI alerted Citrix to the possibility that they were compromised and informed Citrix that the hackers had likely used “password spraying” to infiltrate the system. “Password Spraying” is a simple but effective technique that attempts to access a large volume of employee accounts by using a handful of commonly used passwords.

Citrix disclosed the breach to their customers due to US laws that now require companies to notify affected consumers of any incident that may place their personal or financial data in jeopardy.

Citrix are well known for providing virtual private networking (VPN) software that allows a user to remotely access networks over an encrypted connection. Security researchers however have highlighted that VPN tools are currently being targeted by attackers as they can provide a long-term persistent access to a victim’s systems and target additional systems through their supply chain.

### Google plans to move UK users' accounts outside EU jurisdiction

Prompted by Britain’s exit from the EU, Google is to move its British users’ accounts out of the control of European Union privacy regulators, placing them under U.S. jurisdiction instead. This change will allow British law enforcement easier access to tens of millions of Google users sensitive personal information. The recent Cloud Act in the United States makes it easier for British authorities to obtain data from U.S. companies.

This change in jurisdiction also has the potential to leave the data less secure. The United States has some of the weakest data privacy protections of any major economy, unlike the EU, which has some of the world’s most aggressive data protection rules, the General Data Protection Regulation (GDPR).

Google however has stated in email that “Nothing about our services or our approach to privacy will change, including how we collect or process data, and how we respond to law enforcement demands for users’ information. The protections of the UK GDPR will still apply to these users”. British users will be required to acknowledge new terms of service including the new jurisdiction.

# NZ Incident Response Bulletin

Standard Edition - March 2020

## Our Views:

*This month's theme is "Identity Crime".*

Identity crime (which includes creating false identities) is estimated to cost the New Zealand economy as much as $209 million annually according to the Department of Internal Affairs (DIA) and as many as 133,000 New Zealanders may be victims of identity theft each year.

Identity crimes, which are often committed online and across jurisdictions, are also hard to prosecute and have long term impacts for victims. Identity crime is growing, and it impacts companies and individuals across all areas. Knowledge of how this type of cybercrime is perpetrated and how to protect your identity information is vital for all individuals to remain secure and lower the chances of becoming a victim of identity theft.

For business, identity crime is a bigger problem than just identity theft. Identity crime includes the creation of fake identities, using the details of deceased persons, as well as identity theft. Organisations should be aware of identity crime, both due to the financial risks, and the potential reputational risks involved.

What is Identity Theft?

Identity theft is when someone uses your identity information (facts that establish who you are) and pretends to be you.

Information that may be obtained or stolen and used to establish an identity includes:

- Name
- Date of Birth and Birthplace
- Addresses (physical and email) and Phone Numbers
- Passport and Driver's License Details
- Bank Account Numbers
- Photos and Social Networking Details

How does Identity Theft occur?

The methods used by criminals to steal identity information vary frequently; however, common ways this occurs are as follows:

1. Information is given away freely

   In this scenario, the criminal does not even have to steal anything as many individuals will give away their personal data (often over social networking sites) without understanding the long-term consequences. For someone with ill intent, even a name and date of birth can be used maliciously.

2. Offline

   Offline methods to obtain information include:

   - Dumpster Diving – *Digging through your rubbish or mail in search of statements or personal information*
   - Shoulder Surfing – *Looking over a shoulder to collect passwords/pins*
   - Fake Phone Calls – *Pretending to be a legitimate entity company or individual and tricking the victim into supplying information*
   - Wallet theft – *Theft of your wallet to obtain cards, ID, data.*
   - Skimming – *Using a device attached to an ATM machine to obtain credit or debit card details*
   - Pretexting – *Contacting a business and impersonating a legitimate customer to get login details changed/ obtain password information etc.*
   - Record or document theft – *Physical theft of documents from airports, cafes or bags*
   - Posing as a home buyer – *Using open homes to gain access to information insecurely stored*
   - Fake change of address form – *Fraudulently completing a form to forward mail to another address*

# NZ Incident Response Bulletin

Standard Edition - March 2020

3. Online Methods

   Online methods to obtain information include:

   - Phishing/Smishing and Spear Phishing – *using phoney emails, text messages and fake websites to trick the victim into supplying information*
   - Hacking – *Exfiltrating data once a system has been breached*
   - Malware – *Using any form of malicious software such as virus, worm, keystroke loggers or spyware*
   - Spam
   - Monitoring unsecured websites or public WiFi to view the data you transfer

Impact of Identity Crime

The implications of identity crime include financial, reputational, emotional and social tolls. In complicated scenarios, identity theft can take many months to resolve. Financial hardship can result from the need to clean up compromised systems and accounts, create new networks and open new accounts. Disputing an identity thief's activity in your credit history, tax declarations or employment records may be necessary. Loss of income from the theft of investment funds and bank accounts may occur.

Reputational damage can be severe as a criminal can commit offences in your name or your business name that directly harm your reputation and can be time-consuming to fix.

Victims of this type of crime also suffer social and emotional impacts that ultimately impact their personal lives and can also affect workplace productivity. An Identify Theft Resource Centre survey found that 23% of ID theft victims feared for their safety and many suffered an inability to focus, sleep issues and physical illness as a result. 10% were unable to continue working during this period.

How to protect yourself?

Controlling the amount of information you release publicly can reduce the chance of identity theft. Additionally, as thieves may not use any information they steal for months or even years after obtaining it, the need for constant vigilance is required.

- Be careful with whom you share your information and limit the amount you share whenever possible
- Always ask why a business or individual needs any information requested and how they intend to use it before supplying it to them
- Securely store important documents such as your passport or birth certificate (this includes securing electronic copies adequately)
- Do not use public Wi-Fi or a shared computer for online banking or sending any sensitive information or documents
- Do not overshare on social media
- Be suspicious of unexpected events such as unusual bank account activity or unusual letters from creditors
- Request a regular credit report
- Request an access report from Births Deaths and Marriages at the DIA to see who has applied to view your records
- Keep antivirus protection up to date

What to do if you are a victim of Identity Theft?

If you suspect someone is using your identity fraudulently, you should first contact the police. Individual organisations such as your bank and the Department of Internal Affairs may also need to be informed to prevent any further fraudulent activity.

The Department of Internal Affairs has an Identity Theft Online Checklist you can refer to for specific advice. Further resources and information can also be found at the links below:

- New Zealand Police Tips
- CERT NZ – Online Identity Theft
- Department of Internal Affairs Identity Theft Checklist

# NZ Incident Response Bulletin

Standard Edition - March 2020

## Upcoming Events:

| Date | Event | Location |
|---|---|---|
| 26 March 2020 | Cyber Security: The Good, The Bad and the Ugly | Victoria University of Wellington School of Business |
| 31 March 2020 | Future of Security Auckland | Hilton, Auckland |
| 14 – 16 July 2020 | RSA Conference 2020 Asia Pacific & Japan | Singapore |

## 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: