NZ Incident Response Bulletin

Standard Edition – October 2022 – Issue #45

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

More Kiwis Falling Victim To Scams Than Ever

More New Zealanders are falling victim to scams than ever, according to new research from Bank of New Zealand (BNZ). In the last year, four in five people have been targeted by a scam and more than a quarter have fallen victim to one, up seven percent on the year prior. Businesses are also feeling the brunt with 47 per cent of them falling victim in the last year, up from 21 per cent the year prior.

NZSIS, GCSB Minister to visit all Five Eyes partners

Minister for NZSIS and GCSB Andrew Little is set to visit all four other members of the Five Eyes intelligence partnership. His visit includes Canberra, Washington, Ottawa and London, meeting with counterparts and intelligence committee members, visiting agency headquarters, and attending the Billington Cyber Security Summit. In a statement, he said face-to-face contact after the resumption of international travel would reinforce the partnership at a time of global instability and geostrategic competition.

'Massive Social Experiment' Leading To Cyber Hate Says Expert

The internet has changed how we relate and communicate in unimaginable ways, says University of Canterbury (UC) Associate Professor Mike Grimshaw in a new web series about cyber hate and freedom of speech in Aotearoa. "We are living in the middle of a massive social experiment we haven't really thought through; if it was a 'real experiment' or 'research project' it never would have received Human Ethics approval," Associate Professor Grimshaw says. A lecturer in the sociology of religion, diversity and identity, Associate Professor Grimshaw recently edited a special collection for Springer Nature Social Sciences on Digital Hate and (Anti) Social Media. He was approached by Community of Strangers to join the project, which explores the corrosive impact of cyber hate.

Patrick Gower: On Cyber Crime

Let's face it, we're all reliant on the internet and, unfortunately, the more time we spend online - the more time we're open to attacks from cybercriminals. Newshub national correspondent Patrick Gower's new documentary On Cyber Crime premieres on TV Three.

RBNZ completes recommended steps following 2020 cyber attack

New Zealand's Privacy Commission said on Thursday the nation's central bank had made all the changes recommended after it was hit by a cyber-attack in December 2020. In December 2020, the Reserve Bank of New Zealand was the victim of a cyber-attack on the third-party file sharing application it used to share and store information.

The Office of the Privacy Commissioner, a government organisation tasked with improving how personal information is treated, issued a notice to the RBNZ for not meeting its obligations under the privacy act. "The RBNZ has made every change recommended and more, and we are closing this compliance notice confident that all identified areas of concern have been addressed," said Privacy Commissioner Michael Webster.

World

Optus: How a massive data breach has exposed Australia

Australian telecommunications giant Optus revealed about 10 million customers - about 40% of the population - had personal data stolen in what it calls a cyber-attack. Some experts say it may be the worst data breach in Australia's history. This week has seen more dramatic and messy developments - including ransom threats, tense public exchanges and scrutiny over whether this constituted a "hack" at all. It has also ignited critical questions about how Australia handles data and privacy.

Commonwealth experts meet in Singapore to explore solutions to increasing cyber risks in Asia

On 20-21 September, the Commonwealth Secretariat held a conference on addressing cybercrime in Asia, which saw law enforcement officials, prosecutors, judges and magistrates, key domestic policymakers, international security experts, and academics deliberate on solutions to the region's growing cybercrime and cybersecurity challenges. The conference was prompted by increasing internet penetration rates and the rapid adoption of digital technologies, which have brought immense benefits to the Asia region while increasing its vulnerability to cybercrime and cybersecurity risks.

Cybersecurity threats finance sector facing more cunning

Despite Payment Card Industry Data Security Standard compliance improving significantly in 2020, the cybersecurity threats organisations face are more cunning and evasive than they were even two years ago, according to the 2022 Verizon Payment Security Report. This year's report found that, overall, PCI DSS compliance improved significantly in 2020, with 43.4% of organisations maintaining full compliance, compared to 27.9% in 2019. Additionally, while over half (56.7%) of organisations failed their interim validation assessment due to one or more security controls omissions, the security control gap still improved substantially, from a high 7.7% in 2019 to a low 4% in 2020.

Cyberattack Costs for US Businesses up by 80%

In seven out of eight countries, cyberattacks are now seen as the biggest risk to business — outranking COVID-19, economic turmoil, skills shortages, and other issues. The "Hiscox Cyber Readiness Report 2022," which assesses how prepared businesses are to fight back against cyber incidents and breaches, polled more than 5,000 corporate cybersecurity professionals in the US, UK, Belgium, France, Germany, Ireland, Spain, and the Netherlands. These experts had some enlightening things to say.

UK police arrest teenager suspected of Uber, GTA 6 hacks

Police in London have confirmed a 17-year-old teenager, who is suspected of involvement in high-profile breaches at ride-hailing giant Uber and Rockstar Games, has been charged with multiple counts of computer misuse and breaches of bail. The suspect, whose name was not released due to U.K. reporting restrictions on identifying non-adults, was arrested in Oxfordshire on September 22 as part of an investigation by the City of London Police, which primarily focuses on financial crimes, and is supported by the U.K.'s National Crime Agency.

Hackers Aid Protests Against Iranian Government with Proxies, Leaks and Hacks

Several hacktivist groups are using Telegram and other tools to aid anti-government protests in Iran to bypass regime censorship restrictions amid ongoing unrest in the country following the death of Mahsa Amini in custody. "Key activities are data leaking and selling, including officials' phone numbers and emails, and maps of sensitive locations," Israeli cybersecurity firm Check Point said in a new report. The company said it has also witnessed sharing of proxies and open VPN servers to get around censorship and reports on the internet status in the country, with one group helping the anti-government demonstrators access social media sites.

U.S. Charges 3 Iranian Hackers and Sanctions Several Others Over Ransomware Attacks

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) on Wednesday announced sweeping sanctions against ten individuals and two entities backed by Iran's Islamic Revolutionary Guard Corps (IRGC) for their involvement in ransomware attacks at least since October 2020. The agency said the cyber activity mounted by the individuals is partially attributable to intrusion sets tracked under the names APT35, Charming Kitten, Nemesis Kitten, Phosphorus, and TunnelVision.

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.

30/09/2022 – Microsoft Releases Guidance on Zero-Day Vulnerabilities in Microsoft Exchange Server

Our Views:

Cyber Security Budgeting

Budgeting for cybersecurity is challenging partly because increasing and improving your cybersecurity posture is a continuous process rather than a finite task or one-off purchase. There are various ways to tackle cyber budgeting, including setting a percentage of overall IT spend, benchmarking, and taking a risk-based approach.

Some reports indicate that many international businesses set aside about ten per cent of the total IT budget on cybersecurity. This is an interesting ballpark figure, but a percentage does nothing to guarantee that critical cyber risks can be addressed or managed within risk tolerance. Some businesses may achieve acceptable cyber risk management for less than ten per cent of the IT spend. In contrast, others may have a large and high-risk environment requiring significantly more spending on security.

Therefore, more mature organisations may start budgeting by putting aside percentages and using a risk-first approach. This involves assessing your current risk levels and determining what is needed to address these. When evaluating cyber risks and determining budget allocation, the main points for consideration tend to fall into People, Processes and Technology categories. However, in each of these areas, some unique environmental issues will challenge the cybersecurity budgeting process through 2022 and 2023.

People

Technology is only as good as the people configuring, driving, monitoring and using it. Therefore, investing in skilled IT resources that know how to mitigate and respond to threats should not be overlooked. In the following year, the impact of rising inflation combined with scarce cybersecurity resources may contribute to a need for increased spending to secure talented professionals.

Additionally, the human factor plays a crucial role in most cyberattacks, and this trend is not showing any indication of changing this year; therefore, considering investing in comprehensive training and awareness for all technology users within a business makes sense over the coming months.

Process

Procedures for basic cyber hygiene such as solid backup creation, device hardening, incident response and crisis management must be implemented, documented, understood, and tested for effective protection. Creating, maintaining and testing these processes that secure your assets requires budget consideration.

Changing regulatory requirements also drive the need for a budget in this area. For example, strengthened privacy legislation has led to a need for documented procedures to ensure compliance with Privacy Act obligations, such as mandatory notification. The grace period for this change is over, and all businesses must invest in appropriate processes to address this. In addition, companies that operate internationally may have further compliance measures to implement, including data classification and data lifecycle management.

Ensuring cyber governance procedures are in place also requires funding for establishment and maintenance. Governance procedures include risk assessment processes that help evaluate what kind of attack your business is likely to suffer and what impact this may have on your high-value assets, ultimately helping you to invest in the right areas.

Technology

There is an overwhelming plethora of technology solutions and tools available for purchase in the cybersecurity market. This means there are excellent options for protecting and monitoring your environment, but it also opens up the opportunity for overspending in this space. Understanding which tools will address your critical risks and budgeting for those, rather than relying on vendor sales pitches, is key to maintaining the right level of spending in this area.

The changing threat landscape in 2022 and 2023 should also be reviewed when considering technology investment. Vulnerabilities from increased cloud adoption, increased number of endpoints and more external exposure may require focus. Increasingly businesses will need to put significantly higher levels of effort into managing the cyberhealth of external parties.

The geopolitical environment, notably the war between Russia and Ukraine, has already altered the cyber threat landscape globally this year. Moreover, it will likely continue influencing threat levels for specific industries and subsequent cybersecurity budgeting. Securing industrial environments may also need to be prioritised due to increased convergence between corporate IT systems and operation control systems.

While not neatly fitting into the above categories, changes to the costs of your cyber insurance policy may also need to be factored in over the next year.

Finally, don't forget to expect the unexpected and allow for additional spending, over and above your current budget, particularly if you suffer a cyber incident.

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: