NZ Incident Response Bulletin

Standard Edition – August 2022 – Issue #43

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

'Too much she'll be right' on cyber resilience

David Clark, the minister for all things cyber, says record investment in New Zealand's online resilience comes as cybercrime becomes an increasingly common experience. Budget 2022 saw more than $30 million directed towards cyber initiatives, including a one-stop shop for reporting cyber incidents and cash for victims of cybercrime. The initiative that may make the largest difference in the long term is the modestly-named "cyber resilience measurement framework". This effort to quantify New Zealand's cyber resilience could lay the foundation for starting to improve it. The world-first framework will take an expansive view of what it means to be cyber resilient and try to find ways to measure each of those aspects. That could range from the amount of money lost to cybercrime in the past quarter, to the uptake of security patches, to how comfortable people report feeling in their online transactions.

Security tool will help protect against 'quantum' hackers

A security tool picked up by the US Government is based on Auckland University research and will help protect against cyber attacks from "quantum" hackers. Crystals-Dilithium is the name of one of four "quantum-resistant encryption systems" approved for use by the US National Institute of Standards and Technology last week. "Quantum-resistant encryption" refers to security systems that can withstand attacks by quantum computers - a new generation of computers, hundreds of million times more powerful than the most advanced supercomputers today. The system was built on research co-authored by Professor Steven Galbraith, Head of the Department of Mathematics at Auckland University.

Current cryptography methods rely on mathematical algorithms so complicated that even supercomputers would take millennia to solve, but the advance and wider accessibility of quantum computers would make this redundant. In 2019, an algorithm expected to take IBM's supercomputer Summit 10,000 years to compute was completed in a mere 200 seconds by Google's quantum computer.

How secure is accounting software data in Aotearoa?

A Xero study released in December 2021 found that ICT spending for New Zealand businesses has seen a significant increase compared to pre-pandemic levels. The study, titled 'Picking up the pace: Trends in small business technology adoption and use', gathered anonymous data from more than 300,000 small businesses across New Zealand, Australia and the UK and factored in statistics involving aspects such as digitisation practices, app use, economic growth rates and total expenditure. New Zealand enterprises have increased their ICT spending by 25%. In contrast, the UK has increased by 20% and Australia by 13%. Although both the UK and Australia had higher expenditure rates in individual categories within the data, New Zealand came out on top overall. "This demonstrates that small businesses in New Zealand, as well as Australia and the UK, are embracing technology to adapt to a changing operating environment and realising the benefits that cloud accounting and digital tools provide," Xero says, citing the research.

According to their website, small businesses, contractors, and those who are self-employed all need to keep their tax records for a minimum of seven years in the event they are audited and required to share them with Inland Revenue. Records that need to be kept include invoices, receipts, petty cash, vehicle logbooks, wage books, banking records, asset registers and depreciation schedules, and emails arranging business meetings if travel expenses to another city or country are part of a claim. This means that the data at risk of being stolen doesn't just have to be recent, potentially exposing businesses to data breaches dating back years. Combining this with the increased uptake, it's worth asking, how secure is accounting software data? Xero says that ultimately, accessing accounting software from a greater number of devices and locations will bring increased risks of login information being intercepted by malware. "This risk can be mitigated by only ever logging in from a known device, and having two factor authentication set up on all services," Xero says.

World

Ransomware attacks on education institutions increase

Education institutions are increasingly being hit with ransomware, with 60% suffering attacks in 2021 compared to 44% in 2020, according to Sophos. Sophos has published a new sectoral survey report, The State of Ransomware in Education 2022. The findings reveal that education institutions faced the highest data encryption rate (73%) compared to other sectors (65%), and the longest recovery time, with 7% taking at least three months to recover almost double the average time for other sectors (4%). Additional findings include:

- Education institutions report the highest propensity to experience operational and commercial impacts from ransomware attacks compared to other sectors;
- Only 2% of education institutions recovered all of their encrypted data after paying a ransom (down from 4% in 2020); schools, on average, were able to recover 62% of encrypted data after paying ransoms (down from 68% in 2020);
- Higher education institutions in particular report the longest ransomware recovery time; while 40% say it takes at least one month to recover (20% for other sectors), 9% report it takes three to six months.

These ransomware hackers gave up when they hit multi-factor authentication

A ransomware attack was prevented just because the intended victim was using multi-factor authentication (MFA) and the attackers decided it wasn't worth the effort to attempt to bypass it. It's often said that using MFA, also known as two-factor authentication (2FA), is one of the best things you can do to help protect your accounts and computer networks from cyberattacks because it creates an effective barrier – and now Europol has seen this in action while investigating ransomware gangs.

"We've done investigations where ransomware criminals were monitored. In certain investigations, we saw them trying to access companies – but as soon as they would hit two-factor authentication in this process, they would immediately drop this victim and go to the next," said Marijn Schuurbiers, head of operations at Europol's European Cybercrime Centre (EC3), speaking about an undisclosed incident the agency investigated. It demonstrates how useful MFA can be in preventing ransomware and other cyberattacks. Even if the attacker has the legitimate password for the account – either because it's been guessed or it's been stolen – using MFA usually prevents them from being able to log in.

Ransom payments fall as fewer victims choose to pay hackers

Ransomware statistics from the second quarter of the year show that the ransoms paid to extortionists have dropped in value, a trend that continues since the last quarter of 2021. Ransomware remediation firm Coveware has published a report today with ransomware data from the second quarter of 2022 showing that although the average payment increased, the median value recorded a significant drop.

In Q2 2022, the average ransom payment was $228,125 (up by 8% from Q1 '22). However, the median ransom payment was $36,360, a steep fall of 51% compared to the previous quarter. "This trend reflects the shift of RaaS affiliates and developers towards the mid-market where the risk to reward profile of attack is more consistent and less risky than high profile attacks," comments Coveware in the report. The median size of the companies targeted this quarter dropped even further, with the actors looking for smaller yet financially healthy organizations to disrupt, the company says.

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 our YouTube Channel and this webpage.

Alerts

18/07/2022 – CISA Updates Advisory on Cyber Actors Continued Exploitation of Log4Shell in VMware Horizon Systems

Our Views:

Staying up to date with cybersecurity

Staying on top of contemporary cybersecurity developments and cyber threat intelligence can be hard – even when cybersecurity is your primary role. Understanding the best methods to keep safe, how to recognise the latest scams, which industries have recently been breached, and what the latest product advancements are can be overwhelming.

Due to the escalating nature of cyber-attacks and their increasingly harmful impacts, the subject of cyber security is now discussed in numerous blogs, news reports, magazines and networking channels. Every day, new information on significant breaches and sophisticated scams is posted and marketing material on the latest security technology floods our inboxes.

This fast-moving landscape and 24-hour news cycle can make it almost impossible to keep up with all the cyber information out there leading to cyber security fatigue, weariness and even apathy in light of the constant barrage. Finding efficient, reliable and reputable sources and ways to ensure your knowledge is up to date however is critical.

Actions you can take to stay on top

1. Attend live events and conferences

Attending regular in-person, live cybersecurity events, such as the recently held NZ Cyber Security Summit, that incorporate seminars, lectures, workshops, education and networking can be a great way to give full attention to the topic, download the latest updates across the cybersecurity arena and make key contacts for further information.

Web-based activities, such as webinars and conference calls, can be another option. Many of these events attract the top live cybersecurity speakers, who share insights and valuable up-to-date knowledge that otherwise would not be written down.

2. Follow security specialists and influencers

Following top security experts who blog regularly can be a good way to hear the insider's take on developing situations. Some of the most well-known experts to consider include:

- Bruce Schneier
- Brian Krebs
- Richard Bejtlich
- Magdalena Chelly

And a bit closer to home…

https://www.privacy.org.nz/blog/

3. Monitor vulnerability and risk advisory sites

We recommend and provide links to various reputable threat advisory sites in this bulletin. Subscribe to these and set an alert or regular calendar appointment to regularly scan these for updates.

4. Consider podcasts

Podcasts can be ideal for filling the time during your daily commute, when travelling, or even while exercising (when reading an article may not be an option). Spotify, Amazon, YouTube and iTunes all offer cybersecurity-related content.

5. Consider setting up real-time notifications

Popular forums such as the subreddit/netsec often include great information on cybersecurity topics. Consider customising these sites to deliver notifications as appropriate such as when a topic gets popular.

6. Commit to a yearly training course

Many organizations provide training courses for cybersecurity professionals and committing to a yearly course may be a way to not only stay on top, but ensure your enthusiasm and drive for cybersecurity remains high. It is easy to get burnt out in an industry where it often feels like we are one step behind the "baddies". Investing in yourself to learn a new skill may reignite your passion or open up a new, parallel career path.

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: