NZ Incident Response Bulletin

Standard Edition – July 2021

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.

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

Prime Minister Jacinda Ardern says global effort needed to confront cyber attacks

Prime Minister Jacinda Ardern says a global effort to combat the rise in cyberattacks is needed, as US President Joe Biden confronts Russia's Vladimir Putin over the harbouring of malicious hackers. Ardern, in a discussion with members of the influential US think tank Council on Foreign Relations (CFR), said the recent Waikato District Health Board ransomware attack showed "how devastating" such attacks could be. "Cybersecurity is a space where New Zealand and the United States have been working together. But I think building multilateral architecture in this space would be important, as will be the enforcement because actually it's often hard for us to identify when things are being perpetrated by state actors," she said.

Cyber security breach reports rise by 25%

The number of cyber security incidents reported in this country has risen 25 percent since the same time last year. Government agency CERT NZ's quarterly report shows there have been 1,431 cyber security incidents in the first quarter of this year. Though there was a year-on-year increase, the number was a fall from the last quarter of 2020 when there were 2,097 breaches. The financial loss due to the cyber incidents rose by seven percent. Almost a quarter of the breaches resulted in financial loss, totalling $3 million. Six cases involved losses of $100,000 or more. Of the incidents, 278 were referred to police - an increase of 46 percent compared to the previous quarter.

Dealing with cyber criminals: Some NZ businesses 'feel they have no choice but to pay'

An increasing number of New Zealand businesses are paying ransoms to cyber criminals. The founder of forensic technology and cybersecurity company Incident Response Solutions, Campbell McKenzie, said some of his clients were so paralysed by ransomware attacks they felt they have no choice but to pay. "You have those that would just never in a million years pay a ransom because you're paying money to a criminal group. And then you have those that are essentially facing an existential threat, because they've lost all of their data and can't do business, and feel they have no choice but to pay."

OPC sends warnings to organisations to get it right next time

In recent weeks, the Office of the Privacy Commissioner has been contacting individual organisations about specific privacy breaches that have been raised with them. They state that they are taking a more proactive approach to remind and warn individual organisations of their statutory responsibilities under the Privacy Act 2020.

Authorities blind to size of cybercrime problem

Cybercrimes are on the rise, but authorities are blind to just how big the problem is. There are more than a dozen government agencies and other groups who report, analyse and fight cyber-attacks here, but critics say no one is looking at the big picture, and victims often don't know who to turn for help.

NZ Incident Response Bulletin

Standard Edition – July 2021

World

World's biggest meat producer JBS pays $11m cybercrime ransom

JBS, the world's biggest meat producer, has paid an $11 Million ransom after a cyber-attack shut down operations, including abattoirs in the US, Australia and Canada. While most of its operations have been restored, the Brazilian-headquartered company said it hoped the payment would head off any further complications including data theft. JBS, which supplies more than a fifth of all beef in the US, reportedly made the payment in bitcoin.

Sensitive medical, financial data exposed in extortion of Massachusetts hospital

A hospital in Massachusetts quietly paid off a ransomware gang after a February hack that exposed patients' sensitive medical and financial data, the hospital said in a May 28 statement. Sturdy Memorial Hospital, a 126-bed facility in the city of Attleboro, said that the information exposed in the hacking incident may have included insurance claim numbers, medical history, treatment information, Social Security numbers, bank routing numbers and credit card numbers and security codes, among other data.

Ukraine arrests ransomware gang in global cyber criminal crackdown

Ukranian police have raided the headquarters of the notorious Clop ransomware gang, seizing computer hardware used in its operations along with the equivalent of $184,000, which is most likely ransom money. According to Cybernews, the group has attacked several high-profile targets mostly in the US, and South Korea, including the Stanford University Medical School, the University of Maryland, and the University of California. Clop was also reportedly adept at running a ransomware-as-a-service operation and had collaborated with other cybercriminal groups, especially when going after bigger targets such as oil giant Shell, and the American Flagstar Bank.

Most firms face second ransomware attack after paying off first

Some 80% of businesses that choose to pay to regain access to their encrypted systems, experience a subsequent ransomware attack, amongst which 46% believe it to be caused by the same attackers.

Breached companies facing higher interest rates and steeper collateral requirements

Companies are now being penalised financially by banks for data breaches, according to a new study from the American Accounting Association. In a new report, titled "Do Banks Price Firms' Data Breaches?" the organisation found that banks are punishing companies that lose customer financial account information or social security numbers through data breaches with substantially higher interest rates and steeper requirements for collateral and covenants.

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

24 June 2021 CISA – Bad Practices

4 June 2021 – CISA - Unpatched VMware vCenter Software

News Clips

21 June 2021 - Former hacker warns against 'worse' cyber attacks aimed at US

NZ Incident Response Bulletin

Standard Edition – July 2021

Our Views:

This month's theme is "Cyber Controls # 1 to 3".

Version 8 of the Centre for Internet Security (CIS) controls was released in May 2021, consisting of 18 top-level controls and 153 safeguards (sub controls) that can guide you through the process of creating a layered or defence-in-depth cybersecurity strategy. In this month's bulletin, we take a deep dive into the first three controls, why we need them and ways to implement them. The first three controls in the CIS set are not seen as the "sexiest" cybersecurity actions available, however they are numbers 1 to 3 for a reason. In addition to reducing cyber threats, they serve as a critical foundation for many of the other controls. The NIST Cybersecurity framework also recognises these controls as priority 1 actions and we would recommend these as a strong place to begin any cybersecurity improvement programme.

CIS Control 1: Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorised and unmanaged assets to remove or remediate.

Why is it needed?

You cannot protect what you do not know is there. Essentially this control emphasises the need for visibility of what an enterprise has on its network. Cyber attackers are constantly scanning the Internet address space of target organisations to look for unprotected assets attached to a network. They target assets that are not securely configured or patched and are susceptible to malware, to gain access.

Controlling enterprise assets can be challenging due to the size and dynamic nature of large networks with portable devices connecting only periodically. Additionally, cloud-based, and virtual machines can be paused or shut down making them difficult to track. The managed control of all enterprise assets will however assist with vital tasks such as security monitoring, back up, incident response and recovery.

How is it implemented?

Meeting this control requires the ability to track and correct asset permissions. Technical and procedural actions are combined to create a formal inventory management process. Asset owners should be identified to ensure governance of the process.

Larger organisations may opt for comprehensive commercial products to manage asset inventory, whereas smaller businesses can use existing tools and manage the outputs in a database or spreadsheet. A discovery scan of the network can be undertaken using a vulnerability scanner and this data combined with data from the review of anti-virus logs, switch network logs, authentication logs and endpoint security logs to gain a comprehensive baseline inventory. Other sources of data may include purchase order tracking and local inventory lists.

Maintaining this inventory is an ongoing and dynamic process requiring scanning on a regular basis, sending various packet types across the network to identify assets. Where possible organisations should collect data from enterprise systems such as Active Directory, Single Sign-on, Multifactor Authentication, Virtual Private Networks, Intrusion Detection Systems, Mobile Device Management and Vulnerability Scanning.

The basic level of this control involves two safeguards: Establishing and Maintaining Asset Inventory as described in the steps above. The second safeguard however requires addressing unauthorised assets on the network. This involves a weekly process for removing or quarantining unauthorised assets or denying remote connection of them to your network. Access control could use existing network technology to limit device access to networks.

After the two safeguards above are established, an organisation can consider more advanced sub-controls such as using an active discovery tool, using Dynamic Host Configuration Protocol (DHCP) logging to update the inventory, and using a passive discovery tool.

NZ Incident Response Bulletin

Standard Edition – July 2021

CIS Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorised software is installed and can execute, and that unauthorised and unmanaged software is found and prevented from installation or execution.

Why is it needed?

This control highlights the need for awareness of what software is running on your network and the ability for finding unauthorised or unmanaged software to prevent its installation and use. Attackers scan networks looking for vulnerable software versions that can be exploited. Whilst patching software is critical to preventing these attacks, if a business is not aware of vulnerable software this cannot be addressed. Hence a comprehensive software inventory is critical for preventing cyberattacks.

Understanding the software on your network also allows for more effective cyber risk management. A review of your software inventory list may uncover software that is unnecessary for business operations and can be removed thereby reducing the attack surface. If an incident occurs, having a software inventory will also reduce the work and timeframe required to uncover the potential damage a breach may have caused.

How is it implemented?

We recommend that before any other steps are taken in this control, that organisations limit local administrator rights and installation rights. This will help reduce the amount of unauthorised or unmanaged software that will require removal. Commercial tools for software inventory are widely available and check for commonly used enterprise software. These tools also identify the patch level of each installed program to ensure they are up to date and can be utilised to create an initial software inventory.

When managing this software inventory, the implementation of allowlisting can be used. Whitelisting and blacklisting can be introduced in stages, starting with a list of "unauthorised" applications commonly called a "blacklist". A list of authorised applications then makes up the "whitelist". This process should be documented as a policy and followed up with scanning, and removal of unauthorised software. Contemporary endpoint security solutions often support allowlisting, as do many operating system versions. Some even allow custom allowlists that determine whether an application should be run based on executable path, hash, or regular expression matching.

The basic safeguards that any business must implement in this control include the establishment and maintenance of a software inventory, removing unauthorised software from the network monthly, and ensuring authorised software is currently supported. More advanced safeguard steps include using automated inventory tools, implementing allowlisting of software and libraries and scripts.

CIS Control 3: Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Why is it needed?

Data privacy is increasingly important and there are now numerous international regulations for the protection of data. Data can be difficult to manage as it exists on the cloud, in end-user devices, at home, and is often shared with partners and online service providers. If data is not managed appropriately throughout its lifecycle, there are significant financial and reputational risks to a business.

Once an attacker successfully gains access to a network, a key goal is then to find and exfiltrate data. Depending on the nature of the data this is then used for a wide range of criminal activity such as espionage, ransom, identity theft, or blackmail. Unfortunately, businesses are often unaware that an attacker has breached their network or that sensitive data is being taken until after the fact as data outflow is not monitored. Additionally, whilst data is lost in cybercrime, it is also commonly accidently shared through user error and poor data management.

NZ Incident Response Bulletin

Standard Edition – July 2021

How is it implemented?

Implementing successful data management involves managerial, procedural, and technical actions. Managerial controls consist of policies outlining the type of data the business holds, how it can be used, how it is classified, organised, stored, and how long it is kept. These can be challenging to create as they require executive support and buy-in however they form the baseline understanding of data management in your business and drive all other actions for data lifecycle management. While policy cannot prevent a breach, it does help everyone understand their role in protecting the businesses data. A data breach process should also be developed that links to any cyber incident response plan to ensure fast response and recovery in the event of data breach.

Determining the types of data your business holds can enable effective management. Identifying the sensitivity levels and criticality levels of all data held and defining this using levels or labels such as “Sensitive”, “Confidential” or “Public” can be helpful. Firstly, define the sensitivity and criticality, then create a map of your data describing what applications access and store certain data. This will provide a comprehensive view of how data is used in your business and which critical systems and processes require securing and monitoring.

Procedural controls include performing regular scanning to ensure sensitive information is only stored where is should be and moved or archived when necessary.

Technical controls include ensuring data is encrypted at rest and in transit, blocking access to file transfer, certain email sites and USB ports to prevent exfiltration. These actions can be implemented at little cost. More advanced solutions include Data Loss Protection systems that look for exfiltration attempts utilising deep content inspection and detect any suspicious activity associated with a protected network.

At a basic hygiene level, the CIS controls recommend businesses establish and maintain data management processes, establish and maintain a data inventory, configure access control lists, enforce data retention, securely dispose of data and encrypt all data on end-user devices. More mature businesses with greater security resources can consider actions such as a data classification scheme, documented data flows, encrypting data in all states and locations, segmenting data processing based on sensitivity, deploying a data loss prevention system, and logging sensitive data access.

These first three CIS controls set the stage for an effective cyber security programme. We recommend targeting the implementation of these three at the basic level as a priority in your business.

NZ Incident Response Bulletin

Standard Edition – July 2021

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

Further Resources:

Alerts	Data Breach Response	Forensic Technology
Cyber Incident Simulations	Social Media Investigations	Guide for NZ Law Firms

Share our Bulletin: