National Cyber Security Centre

Cyber Threat Report 2018/19

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government

Contents

Foreword

The National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), helps protect New Zealand's organisations of national significance from advanced cyber threats and responds to cyber incidents that may impact New Zealand's national security and economic wellbeing. This report aims to provide insight into the types of cyber threats and incidents encountered by these organisations this year.

In the financial year from 1 July 2018 to 30 June 2019, the NCSC recorded 339 cyber security incidents, with a "cost avoidance" benefit to nationally significant organisations in the order of NZD27.7 million. Since June 2016, CORTEX capabilities have reduced harm from hostile cyber activity by around NZD94.7 million.

This year, 38% of the NCSC's recorded cyber incidents contained indicators linking them to state-sponsored cyber actors. Of these, a greater proportion were characterised as "post-compromise" compared with the previous year – an indicator of the increasingly serious impact of state-sponsored cyber threats to New Zealand organisations.

The evolution of the NCSC's cyber defence capabilities continues with the expansion of Malware Free Networks, a new cyber threat intelligence capability to disrupt the ability of malware to impact New Zealand.

Since the release of the NCSC's initial Cyber Security Resilience report in 2018, the NCSC has worked with New Zealand organisations to increase cyber security resilience across four key areas: governance, investment, readiness and the technology supply chain. This year, the NCSC noted an increase in self-reported cyber incidents, indicating a growing cyber awareness among New Zealand organisations.

NCSC worked with industry partners to develop voluntary standards for industrial control systems. The industry-driven standards provide a best practice foundation, designed to improve an organisation's cyber resilience and secure the assets critical to the operation of New Zealand's control system environments.

This year also featured the government's launch of the New Zealand Cyber Security Strategy 2019. Along with our partners, NCSC will contribute to the implementation of this strategy.

Internationally, like-minded states introduced tougher requirements for responding to data breaches. These changes aim to increase the security of personal data. New Zealand's privacy legislation is currently under consideration. Legislative reform could change the requirements for New Zealand entities to handle the personal information of New Zealanders and protect it from unintended exposure.

New Zealand's partners and like-minded states are increasingly calling out state-sponsored malicious cyber activity that is counter to international norms of acceptable behaviour in cyberspace, and contrary to norms in the international system. On behalf of the New Zealand Government, the GCSB's Director-General publically attributed malicious cyber campaigns to Russian and Chinese state actors.

The NCSC is uniquely positioned to provide insight into the nature and extent of serious cyber threats targeting New Zealand's nationally significant information and systems. We hope this report will contribute to an increased understanding of the cyber threat environment in which New Zealanders work, play and interact.

Lisa Fong
Director, National Cyber Security Centre

About the National Cyber Security Centre

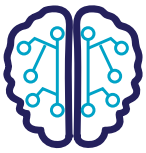
The GCSB's National Cyber Security Centre plays a vital role in protecting government agencies and New Zealand's nationally significant organisations from cyber threats with the potential to affect New Zealand's national security and economic wellbeing.

The NCSC provides detection and disruption services, as well as specialist information security services, advice and support to assist nationally significant organisations. Our customers include government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

Cyber defence

The NCSC operates a suite of cyber defence capabilities developed as part of the CORTEX initiative, and provides incident response support to help nationally significant organisations address potentially high impact cyber events.

The NCSC has primary responsibility for responding to state-sponsored cyber threats, or for cyber security threats that may affect New Zealand's national security and economic wellbeing. One of our key focus areas is countering advanced, persistent cyber threats, which are typically beyond the detection and disruption capabilities of commercial products and vendors due to their sophisticated nature.



CORTEX

Throughout 2018/19, the NCSC continued to improve CORTEX capabilities to best support nationally significant organisations. CORTEX is not a "one size fits all" model, but a range of capabilities that can be deployed at different points on a customer's network depending on network configuration and risk profile. Some services provide alerting when specific activities are detected on a network, while others actively disrupt malicious activity.

The concept behind CORTEX is more than just direct cyber threat detection and disruption. If we know activity is targeting one customer's network, we can make that cyber threat information available to a much wider group.

This enables organisations not directly protected by CORTEX, or that have not yet been targeted, to mitigate the threat. This is the premise behind the development of the NCSC's newest capability, Malware Free Networks.

Analysis undertaken by the GCSB shows that in 2018/19, the detection and disruption of malicious cyber activity through CORTEX capabilities prevented NZD27.7 million in harm to New Zealand's nationally significant organisations. Since June 2016, CORTEX capabilities have reduced harm from hostile cyber activity by approximately NZD94.7 million.

In July 2018, the GCSB received the award for **Building Trust and Confidence in Government** from the Institute of Public Administration NZ (IPANZ) for the Project CORTEX cyber security initiative. In November 2018, CORTEX was named **Best Security Project or Initiative** at the 2018 iSANZ (information security) awards.

Malware Free Networks

Malware Free Networks (MFN) is a malware detection and disruption service that involves the NCSC generating and sharing threat intelligence with consenting organisations. The NCSC has worked with a range of customers and network operators to identify the best way to deliver this new service, and to establish the technology platform that will enable the most effective sharing of cyber threat intelligence.

In 2018/19, the MFN capability was successfully piloted with an internet service provider, which saw the GCSB sharing cyber threat information and technology to help mitigate malware for a subset of consenting commercial customers. This kind of cooperation between public and private sector organisations is an important part of our national strategy for increasing New Zealand's cyber resilience. Customers will be able to receive the MFN threat intelligence feed either directly from the NCSC or via their network operator. This approach ensures customers with varying capability levels will be able to receive the benefits of MFN.

Who we work with

In order to effectively protect New Zealand and New Zealanders from advanced cyber threats, the NCSC works closely with its domestic and international partners. The NCSC, CERT NZ (New Zealand's Computer Emergency Response Team), and New Zealand Police work together to ensure the New Zealand Government's response to cyber events is effective and comprehensive.

New Zealand Police is responsible for responding to crimes occurring online, and CERT NZ works to support businesses, organisations and individuals who are affected by cyber security incidents. The NCSC responds to cyber incidents involving organisations of national significance or where there is potential for national impact, for instance to New Zealand's security or economic prosperity.

Te Reo Māori terminology

The New Zealand Government is committed to increasing the use of Te Reo Māori, one of New Zealand's official languages. Here are a few cyber security terms you can learn and use:

Whakahaumaru – *security*

Whakahaumaru ā ipurangi – *cyber security*

Rorohiko – *computer*

Whatunga rorohiko – *network*

Hītinihanga – *phishing*

Pūmanawa kino – *malware*

Whakaraeraetanga – *vulnerability*

Paraketo – *antivirus*

Īmēra – *email*

Kupuhipa – *password*

Pae tukutuku – *website*

The NCSC coordinates a number of regional and sector-based security information exchanges where information security professionals can confidentially share information.

Internationally, the NCSC works closely with the Australian Cyber Security Centre, the United Kingdom's National Cyber Security Centre, the Canadian Centre for Cyber Security, the United States of America's National Security Agency, and the worldwide CERT community, to better understand the international cyber threat environment and provide greater protection to New Zealand organisations.

By the numbers

339

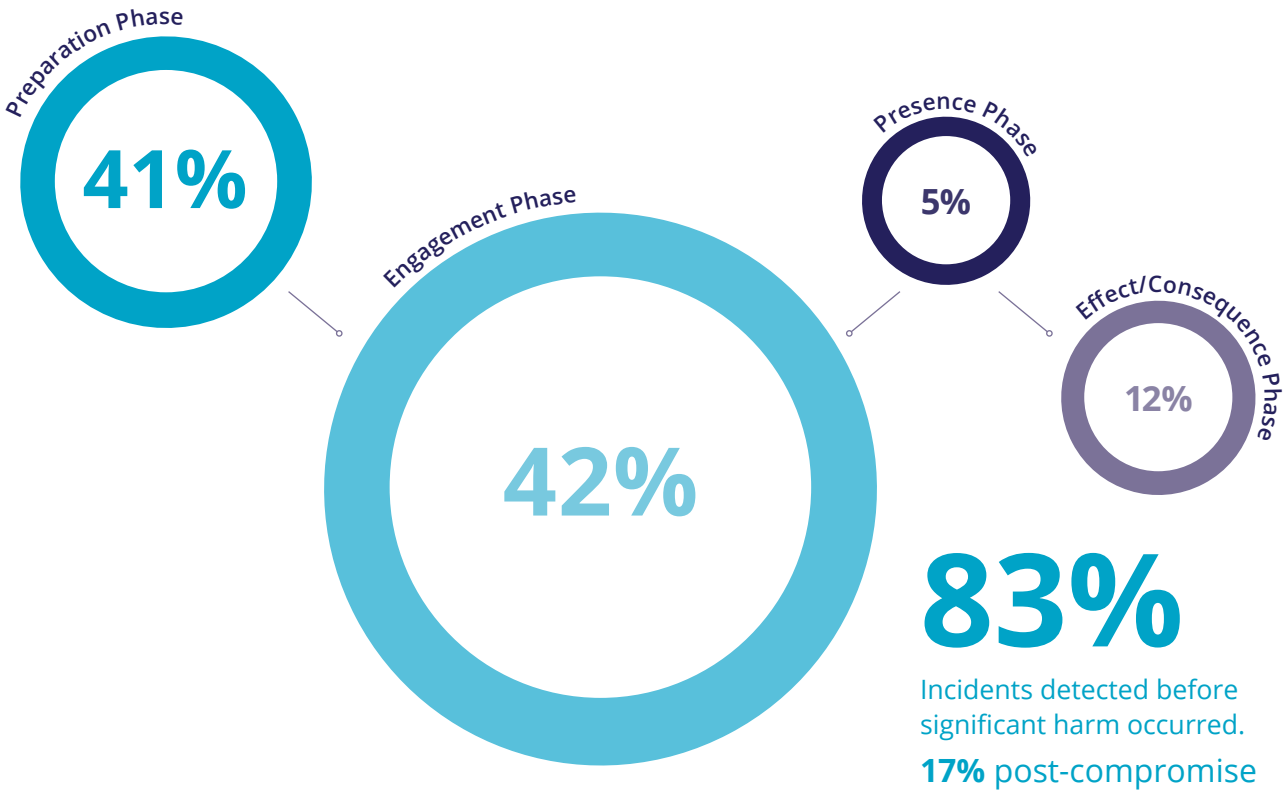
cyber incidents recorded by the NCSC

347 in 2017/18

38%

had indicators of links to state-sponsored actors

39% in 2017/18



83%

Incidents detected before significant harm occurred.

17% post-compromise

In a typical month, the NCSC detects

12 cyber intrusions affecting one or more of New Zealand's nationally significant organisations, through CORTEX capabilities.

16 **new incident reports or requests recieved** for cyber security assistance, unrelated to CORTEX monitoring.

27.7 million

worth of harm

prevented to New Zealand's nationally significant organisations in 2018/19

$94.7 **million** since June 2016

121 security advisories or incident reports disseminated in 2018/19

International cyber threat landscape

State-sponsored and criminal cyber actors continue to target computer systems using the continually evolving range of technologies and tools at their disposal. New technology, products and services aimed at making everyday tasks easier for individuals and businesses can also contribute to the complexity of maintaining security in cyberspace.

International trends and events provide a point of comparison for New Zealand, alert us to future threats, and allow us to prepare for new or emerging types of malicious cyber activity. This knowledge can also help us to understand the broader context surrounding the incidents and activity we have observed in New Zealand.

Public attribution

GCSB continues to work closely with partner agencies across government and internationally to call out malicious cyber campaigns that are counter to internationally accepted norms of behaviour in cyberspace. In 2018/19 the Director-General of GCSB, on behalf of the New Zealand Government, twice attributed campaigns of malicious cyber activity to nation states. These cyber security incidents were designed to generate revenue, disrupt businesses, undermine democracy or facilitate the theft of intellectual property.

In October 2018, GCSB's Director-General publically attributed Russian state actors to a number of malicious cyber campaigns targeting political institutions, businesses, media and sporting organisations. While its primary targets were in the Ukrainian financial, energy and government sectors, its indiscriminate design allowed the campaign to spread around the world affecting these sectors in multiple states.

In December 2018, GCSB's Director-General made a public statement attributing a global campaign of cyber-enabled commercial intellectual property theft to Chinese state actors. The long running campaign targeted the intellectual property and commercial data of a number of global managed service providers, including some operating in New Zealand.

Data breaches

Notable in the international cyber security environment this year was the frequency of public reporting about cyber security incidents resulting in significant data breaches involving personal information. The range of industries impacted includes academia, airlines, hospitality, and social media, and is indicative of the high value of personal information, targeted by both state-sponsored actors and criminals for their own use or to sell for financial gain, or both.

Consequences of data breaches for organisations or impacted individuals can be multifaceted and long-lasting. Organisations involved in data breaches may face reputational damage with customers, potentially resulting in a loss of business. Individuals affected by this type of cyber incident are likely to be at greater risk of being targeted through scams or phishing campaigns in the future, particularly if the data is published on the internet or sold to cyber criminals.

Data breach: the intentional or unintentional release of sensitive or private information into an unsecure environment.

Personally identifiable information: information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.

In response to the increase in significant data breaches, some states have increased regulatory powers and reporting requirements. Following the implementation of the European Union's General Data Protection Regulation in May 2018, several international organisations have received significant fines for data breaches impacting EU citizens.

In July 2019, British Airways and the Marriott hotel chain received fines of £183 million and £99 million respectively.

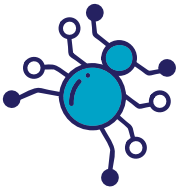
In Australia, new mandatory data breach obligations came into effect in February 2018, replacing the voluntary reporting scheme and resulting in a 712% increase of data breach notifications. New Zealand's privacy legislation is currently under consideration. Legislative reform could change the requirements for New Zealand entities to handle the personal information of New Zealanders and protect it from unintended exposure.

Data breach examples

In August and September 2018, British Airways' website and mobile app were compromised. The financial and personal information of approximately 380,000 individuals was stolen.

In October 2018, airline Cathay Pacific discovered unauthorised access to a system holding the information of up to 9.4 million passengers, including biographic and credit card details, as well as other personal information.

In November 2018, the Marriott hotel chain announced a network compromise that resulted in the data breach of personal information from approximately 383 million guest records. The compromise was undetected for four years before being discovered.



Governments and political parties

Government agencies and political parties remain desirable targets for malicious cyber actors, both state-sponsored and criminal. Motivations for malicious cyber activity targeting government agencies may include state espionage, gaining advantage during international negotiations, disruption of public services, or to draw public attention to political or sensitive issues.

International reports indicate the ongoing interest in the spread of misinformation and attempts to undermine perceptions of democratic processes. This includes incidents against non-government organisations such as Amnesty International, election voter databases, as well as incidents perpetrated by issue-motivated groups. According to analysis from Canada's Communications Security Establishment, in 2018 half of all democracies holding national elections had their democratic process targeted by cyber threat activity.

Examples of malicious cyber incidents observed globally that impacted parliamentarians, elections or political parties this year include the targeting of the Australian Parliament House computer network, as well as some political parties; misinformation campaigns against EU member states; and the discovery of the personal information of hundreds of German politicians published online throughout December 2018. Information obtained included contacts, private chat messages, and financial information including credit card details.

Academia and research institutes

Academia, research institutes, and the science and technology industry continue to be targeted by malicious cyber activity, likely for intellectual property theft or commercial espionage purposes.

Publicly reported cyber security incidents impacting this sector include personal information stolen from prominent universities potentially for use by foreign intelligence agencies in targeting students; sensitive

intellectual property stolen from pharmaceutical companies; and dual-use or military technology stolen from universities and commercial companies, which includes aerospace, bioengineering and naval technology.

Compromising research on advanced technologies or intellectual property can be driven by a need to circumvent legal barriers to legitimate access, such as sanctions or export controls, or to gain commercial or financial advantage.

Vulnerabilities and technology

Malicious cyber actors continue to exploit known, unpatched vulnerabilities in networks, new technologies and smart devices.

Everyday devices with the ability to connect to the internet, also known as the Internet of Things (IoT), continue to pose a risk, potentially exposing the networks they are connected to as well as the devices themselves. Many devices with IoT capabilities are designed for ease of use rather than security, and this technology is becoming increasingly common. IoT capabilities feature in a large range of devices, from TVs and printers, to home alarms and heating systems. Each of these devices can create potential points of vulnerability or access to a variety of data. The challenge for IoT device users is maintaining cyber security awareness while still enjoying the functional benefits the devices offer.

In 2019, security researchers disclosed two vulnerabilities in CISCO routers that could allow a malicious cyber actor to compromise the router, access the data and commands transferring through it, as well as IoT devices connected to the network. Compromised routers can be used to extract intellectual property, maintain persistent access to victim networks, or to conduct malicious cyber activity against another victim.

Technology supply chains will continue to be a point of potential vulnerability to the security of networks, particularly when outsourced information and communications technology service providers have privileged network access.

Malicious cyber actors exploit vulnerabilities in third party supply chain organisations, in order to indirectly target a more secure organisation. The cyber security of one organisation is potentially only as strong as that of the weakest member of the supply chain, which can involve cloud services, third party software providers, and managed service providers.

In one example of this type of risk this year, technology company ASUSTek Computer unintentionally delivered malware through its automated software update system ASUS Live Update Utility. ASUS customers who downloaded software updates unwittingly installed a malicious backdoor onto their own computers. Analysis indicated this supply chain attack lasted for approximately five months, potentially impacting up to half a million systems.

Ransomware remains a threat. Although this year has not featured the same degree of high profile international ransomware incidents such as WannaCry and NotPetya which occurred in 2017/18, the impact ransomware victims experience can be significant. Businesses often must stop operations immediately, either to address the infection or because access to business-critical files or systems has been lost.

Internet of things (IoT): The collective term used for physical devices that are fitted with sensors or software enabling them to be accessed, controlled and monitored remotely. These devices range from household items (heat pumps/light bulbs), to medical devices (pacemakers), and components integral to the operation of critical national infrastructure (power grids/hydroelectric dams/nuclear reactors).

Supply chain: Suppliers or service providers that contribute to or have the opportunity to modify a product or system, during the design, production, distribution, installation or maintenance of the system.

Ransomware: A type of malicious software designed to deny access to a computer system until a ransom is paid.

The New Zealand landscape

Cyber threats to the security of New Zealand's networks continued to grow in scope and scale throughout 2018/19. Malicious cyber actors continue to target New Zealand with a variety of likely motivations, including espionage, illegal revenue-generation, theft of intellectual property and sensitive information, or disruption of nationally significant infrastructure or processes.

The NCSC's work to detect and disrupt those actors has become more important than ever. Both non-state and state-sponsored cyber actors are increasingly sophisticated, as they gain access to more advanced tools and techniques.

NCSC recorded incidents

The NCSC identifies cyber incidents from a number of sources, including detection through its advanced cyber defence capabilities, self-reporting by victims, or reporting from our domestic and international partners. NCSC incidents either involve organisations of national significance, or cyber security threats that may affect New Zealand's national security and economic wellbeing.

During the financial year 2018/19, the NCSC recorded 339 cyber incidents. In a typical month, the NCSC detects 12 cyber intrusions affecting one or more New Zealand organisations through its CORTEX capabilities. In addition, the NCSC receives an average of 16 new incident reports per month, unrelated to CORTEX detection. These are typically self-reported by the impacted organisation, or reported to the NCSC by our international and domestic partner agencies.

Over the last 12 months, incidents have been equally self-reported from private sector organisations and government agencies, indicating an increasing cyber security awareness and maturity among New Zealand organisations.

When a cyber security incident occurs, the NCSC can support the New Zealand victim organisation in several ways. During the 2018/19 year, the NCSC produced 121 reports for customers, alerting them to cyber security incidents or vulnerabilities affecting their networks.

This work included comprehensive forensic investigations into the compromises of New Zealand networks. In these cases, the NCSC worked with the New Zealand victim to assess the extent of the compromise, and provided detailed analysis and remediation advice.

The NCSC also assisted with the response to several high profile issues involving government agencies. These incidents were information management issues rather than the result of malicious cyber activity.

State-sponsored linked incidents

State-sponsored linked activity impacts a variety of New Zealand organisations in multiple industries. Organisations in both the public and private sectors hold a wealth of information that is attractive to other states, from intellectual property for new technology innovations through to customer data, business and pricing strategies or government positions on sensitive topics.

The NCSC assesses New Zealand organisations are facing an increasing risk of successful compromise by state-sponsored actors. During 2018/19, 38% of the NCSC's cyber incidents had links to state-sponsored actors. While this is the same proportion as the previous year, a greater number of state-sponsored linked incidents were characterised as post-compromise.

State-sponsored cyber activity is generally more sophisticated than criminal or non-state activity, a reflection of the greater resources and motivations of the state. This can also increase the difficulty of detecting and mitigating activity.

What is a cyber incident?

The NCSC defines a cyber security incident as an occurrence or activity that appears to have degraded the confidentiality, integrity or availability of data within an information infrastructure.

The NCSC groups incidents into two categories with four phases, for the purpose of analysing the nature and impact of cyber incidents impacting New Zealand:

The **pre-compromise** incident category comprises *preparation* and *engagement* phases.

The **post-compromise** incidents category comprises *presence* and *effect* phases.

CASE STUDY

A New Zealand organisation requested assistance from the NCSC after discovering unauthorised corporate email accounts. In an attempt to avoid detection, the actor created accounts mimicking the names and details of existing personnel. NCSC investigations determined the unauthorised access was linked to a known group of sophisticated cyber actors, who accessed files and email accounts of IT administrators to gain additional access into the organisation's network. The actor also accessed sensitive organisational information, including financial records and emails of executive personnel.

The NCSC worked with the organisation and its service providers to identify the source of the compromise and undertake remediation action.

Regular security audits, penetration testing or vulnerability assessments strengthen an organisation's cyber security, by identifying issues or weaknesses that may not otherwise be recognised. Poor security practices from third party vendors can also increase the potential vectors of compromise a malicious cyber actor can exploit.

Pre-compromise incidents

Pre-compromise activity is characterised by planning and reconnaissance by cyber actors, or initial engagement with their targets. Pre-compromise incidents observed this year include New Zealand organisations that were targeted through phishing campaigns, website compromises, credential harvesting, or brute force attempts. Misconfigured network devices also feature in this category; these may broadcast information such as logins and passwords. Misconfigured devices can create network security vulnerabilities or provide a point of network access that would otherwise not be available to malicious cyber actors.

In 2018/19, 282 NCSC cyber incidents were identified before the point of network compromise. While pre-compromise incidents are lower on the range of severity, they can still have a significant impact on an affected organisation. Pre-compromise activity can evolve into fully fledged network compromise, if not detected and mitigated in a timely manner.

Strengthening the first layer of cyber defence can have a significant impact in protecting an organisation from successful post-compromise cyber incidents.

Post-compromise incidents

The goal of post-compromise incidents is to ensure ongoing access to a network, and to exfiltrate data or disrupt infrastructure or systems. In this financial year, the NCSC managed a greater number of post-compromise incidents than in previous years, representing 17% of incidents. These types of incidents range from internal network reconnaissance and keystroke logging, to encrypting, locking or exfiltration of files. Remediation of incidents that reach the post-compromise phase can have significant impacts for the affected organisation, depending on the nature and extent of the intrusion.

Detection of vulnerabilities

Mitigating known vulnerabilities means cyber actors are forced to use more sophisticated tools and techniques to compromise a network. In 6.7% of incidents this year, the NCSC identified vulnerabilities on New Zealand networks before they were exploited by a cyber actor. In such cases, mitigation advice can be provided to directly affected customers, potentially affected organisations or published as security advisories on the NCSC website.

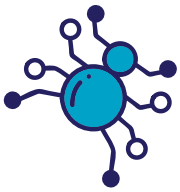
On several occasions this year, the NCSC identified a vulnerability or incident impacting one customer, and was able to provide indicators to a wider set of customers. Such notifications help New Zealand organisations detect potential incidents early, a critical factor in reducing the harm caused by malicious cyber actors.

CASE STUDY

The NCSC became aware of a sophisticated cyber actor exploiting a known vulnerability in a web server software component used by a number of New Zealand organisations. When exploited, actors could install malware to obtain ongoing access to compromised servers. Analysis by the NCSC determined the actor then used this access point to move deeper into the network, by deploying password stealing tools such as Mimikatz or exploiting other vulnerabilities on the wider network.

The NCSC worked with the organisations known to be using the web server software component to identify the scope of the compromise, review the actor's activity, and provide remediation advice to secure the networks.

Out-of-date software remains a key weakness affecting the cyber security of New Zealand organisations. This can be addressed through security patching, and should also include assessing the security of the components included in software products, such as website modules or extensions.



Cyber crime

The NCSC focuses on cyber incidents that are high impact and have national security implications, which includes some instances of cyber crime such as ransomware and business email compromise. In this financial year, 27 of NCSC's cyber incidents contained indicators of criminal activity against public and private sector organisations. These commonly involved the exploitation of unpatched vulnerabilities or lack of multi-factor authentication requirements to access a network, or phishing.

The impact of criminal cyber activity for affected organisations can be reputational as well as financial.

While the financial impact of these techniques can be severe, organisations can manage this risk using a range of technical and internal controls including the use of multi-factor authentication and patching known vulnerabilities. The NCSC has published a General Security Advisory on its website to highlight best practice security steps to protect organisations from the risks associated with business email compromise.

CASE STUDY

The NCSC has assisted a number of organisations this year affected by criminal actors who comprise business email accounts for financial gain. A criminal cyber actor can deceive an organisation's employees into paying significant amounts of money to a bank account controlled by criminals, in the belief they are paying known and trusted entities.

This is often achieved by first targeting the victim organisation through phishing emails, with a link to a legitimate-looking website where the employee is prompted to enter login and password details. The criminal actor uses these credentials to login to the employee's email account and gather information about the organisation's third party relationships or clients. The actor then sends fraudulent invoices, tailored to masquerade as a trusted entity the victim has previously paid. This method allows criminal actors to obtain substantial amounts of money before the suspicions of the organisation are raised.

If multi-factor authentication for remote email access is not enabled, the actor can reuse the credentials and often sets up mailbox rules to forward all incoming emails to an actor-controlled mailbox.

Conclusion

Internet connectivity enables New Zealand to work, play and interact online. Good cyber security is a prerequisite for our economic, social and cultural wellbeing, and for maintaining strong national security.

The benefits New Zealand can receive from the online environment are dependent on an open, trusted internet, and secure infrastructure and technology to support it. We need to know that our systems will keep running, and our personal and commercial information is safe.

This year, the cyber security incidents seen impacting New Zealand's nationally significant organisations have increased in their severity, particularly from sophisticated state-sponsored actors. The greater the severity of an incident, the greater the potential costs to the organisations who are impacted; this may include incident response, network remediation, legal fees or reputational impact. Both state and non-state cyber actors continue to develop and improve their capabilities, and to use a variety of tools to gain access to networks.

As such, it is important for New Zealand organisations to get the basics of cyber security right. This includes patching known vulnerabilities in applications and operating systems, securing critical or sensitive data, and regular security testing. In combination, these actions create layers of cyber defence, making it more difficult for malicious cyber actors to succeed.

The NCSC relies on the consent and cooperation of its customers and the New Zealand public; this is an important part of New Zealand's Cyber Security Strategy to increase New Zealand's resilience against cyber threats. We hope this report will promote informed discussion about cyber security and contribute to increased resilience of New Zealand's nationally significant information systems.

Getting in touch with us

If you have any questions related to this report, please email incidents@ncsc.govt.nz.

If you have encountered a cyber incident, please visit our website for further information: **www.ncsc.govt.nz**

Glossary

Below is a glossary of terms that are included to assist readers' understanding. It should not be interpreted as a comprehensive list of terms used by the NCSC to describe the cyber threat environment.

Advanced Cyber Threat	A well-resourced, highly skilled cyber actor or group that has the time, resources and operational capability for long-term intrusion campaigns. Their goal is typically to covertly compromise a target, and they will persist until they are successful. They are very capable of compromising secured networks using both publically disclosed, as well as self-discovered, vulnerabilities.
Backdoor	A feature or defect of a computer that allows unauthorised access to a device or the data stored on it.
Brute Force	An attempt to guess authentication information such as a password by making multiple attempts in the hope of eventually guessing the correct value.
Credentials	A user's authentication information used to verify identity – typically a password, token or certificate.
Computer Network Defence	A set of processes and measures to protect devices, services and networks – and the information on them – from theft or damage.
Cyberspace	The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.
Cyber Threat	An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.
Exfiltration	Where an actor has unauthorised access to private organisational data (for example legitimate credentials, or intellectual property), and removes it from a system, typically in the form of files, database dump or system memory dump.
Incident	An occurrence or activity that appears to have degraded the confidentiality, integrity or availability of a system or network.
Malicious Cyber Actor	An individual or group of people who seek to exploit computer systems to steal, destroy or degrade an organisation's information. Actors may be individual computer hackers, part of an organised criminal group, or state-sponsored.
Malware	Malicious software or code intended to have an adverse impact on organisations' or individuals' data, e.g. viruses, Trojans or worms.
Mitigation	Steps that organisations and individuals can take to minimise and address cyber security risks.
Router	A network device which sends data packets from one network to another based on the destination IP address.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

New Zealand Government