NATIONAL CYBER SECURITY CENTRE

CYBER THREAT REPORT 2019/20

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

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

Contents

Foreword

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

From 1 July 2019 to 30 June 2020, the NCSC recorded 352 cyber security incidents. Self-reported cyber incidents continue to increase, reflecting the growing cyber awareness and willingness to report incidents among New Zealand organisations. The NCSC's international partners are also increasingly notifying the NCSC about cyber incidents affecting New Zealand organisations, highlighting the value of international partnerships, as well as the transnational nature of activity affecting New Zealand.

The NCSC continues to provide a significant cost avoidance benefit to New Zealand. Over the year, the NCSC provided a cost benefit to New Zealand's nationally significant organisations in the order of $70.5 million. Since June 2016, the NCSC's capabilities reduced harm from malicious cyber activity by around $165.2 million.

The NCSC continues to build and grow New Zealand's cyber defence capabilities, most recently through the successful pilot and initial delivery of Malware Free Networks (MFN). MFN will bring the NCSC's cyber security capabilities to a much larger number of consenting New Zealand organisations.

In response to the global COVID-19 pandemic, the NCSC rapidly changed the way it works to minimise the risk to staff and to maintain continuity of essential services. The NCSC also published cyber security advice and resources to encourage a high level of cyber resilience and awareness throughout the national pandemic response.

During late 2020, a global campaign of denial of service (DoS) events affected a range of New Zealand organisations. These events demonstrated the willingness of cyber actors to carry out persistent malicious activity that has a high national impact. Throughout the activity, the NCSC provided advice to New Zealand's nationally significant organisations.

In addition to responding to cyber threats, the NCSC works proactively with organisations to build their cyber resilience. In the past year, two flagship products about information security governance and incident management were released, and the NCSC contributed to a range of sector-based information sharing forums where sectors enhance collaboration on cyber security challenges.

The NCSC aims to provide unique insight into the nature and extent of serious cyber threats targeting New Zealand's nationally significant organisations. In an increasingly complex and adversarial international cyber environment, the NCSC hopes this report helps to improve the understanding of the cyber threats to New Zealand.

Hamish Beaton
Director, National Cyber Security Centre

Overview

By publishing the Cyber Threat Report 2019/20, the NCSC seeks to increase the understanding our customers and the broader public have about the cyber security threats to New Zealand's nationally significant organisations. This report also aims to promote greater awareness of the work the NCSC does to safeguard New Zealand's nationally significant organisations.

This report covers the NCSC's role as the lead government agency for responding to state-sponsored cyber threats and cyber threats that may affect New Zealand's national security. This includes an overview of some of the NCSC's cyber defence capabilities and services, key areas of work over the 2019/20 fiscal year, and domestic and international relationships.

An overview is also provided about the international cyber threat landscape, with a focus on identifying trends and tradecraft which can inform efforts to defend the New Zealand's nationally significant organisations. This includes malicious cyber activity counter to internationally accepted norms of behaviour in cyberspace, the continued prevalence of data breaches, the exploitation of known vulnerabilities, and the emergence of well-planned ransomware incidents targeting large multinational organisations.

Also provided is a summary of New Zealand's domestic cyber threat landscape, with specific reference to cyber incidents which affected New Zealand's nationally significant organisations. This includes providing insights into some of the ways the NCSC is safeguarding New Zealand's nationally significant organisations from malicious cyber actors of all types.

The report concludes by highlighting what this means for New Zealand's nationally significant organisations, including some straightforward, practical steps organisations – of any size – can take to increase their cyber resilience. Organisations seeking further information about increasing their cyber security and resilience can visit the NCSC website (www.ncsc.govt.nz), where cyber security guidance and resources are regularly shared with the public.

Te Reo Māori terminology

The New Zealand Government, including the GCSB, 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
Aumangea ā ipurangi – cyber resilience
Taihara ā ipurangi – cyber crime
Hītinihanga – phishing
Pūmanawa utu uruhi – ransomware
Whakaraeraetanga – vulnerability
Whakatūturu pārongo – credentials
Raraunga wāwāhi – data breach

By the numbers

41% preparation
42% engagement
7% presence
10% effect/ consequence

30%
had indicators of links to state-sponsored actors
38% IN 2018/19

352
cyber incidents recorded
339 IN 2018/19

83%
incidents detected before significant harm occurred, 17% post-compromise

$70.5 million
worth of harm prevented to New Zealand's nationally significant organisations in 2019/20
$165.2 MILLION SINCE JUNE 2016

82
security advisories or incident reports disseminated in 2019/20

THE NCSC IN A TYPICAL MONTH

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

Receives 18 new incident reports or requests for cyber security assistance, unrelated to the NCSC's CORTEX capabilities

INCREASING CYBER RESILIENCE OVER THE YEAR

Recorded 1,770 engagements with customers

Published 24 reports for general customers

Facilitated 20 regional and sector-based security information exchanges

About the National Cyber Security Centre

The NCSC plays a vital role in protecting New Zealand's government agencies and nationally significant organisations from cyber threats that have the potential to affect national security and economic wellbeing.

The NCSC provides a suite of cyber defence capabilities, as well as specialist information security services, advice and support to assist nationally significant organisations.

NCSC customers include government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

A **cyber threat** is an attempt to undermine, compromise or degrade the function of a computer-based system, access information, or track the online movements of individuals without their permission.

What the NCSC does

As the lead government agency for responding to state-sponsored cyber threats and cyber threats that may affect New Zealand's national security, the NCSC enables the protection, wellbeing and prosperity of New Zealand through trusted information security services.

Analysis undertaken by the GCSB shows that in 2019/20, the detection and disruption of malicious cyber activity through the NCSC's capabilities prevented $70.5 million in harm to New Zealand's nationally significant organisations. While at face value this is a substantial increase relative to previous years, it is largely driven by several factors, including:

Information Assurance and Cyber Security services

Advise by guiding and equipping our customers to protect their valuable information and manage risk. We act as trusted, independent advisors, reducing potential harm for our customers by providing assurance, mitigating risk, enabling innovation, and supporting our customers through security issues.

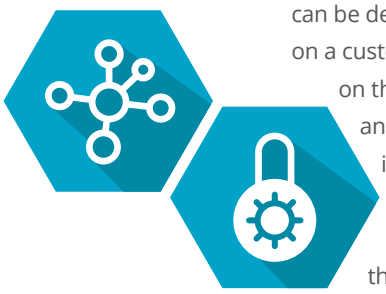
Deter by raising the cost for our adversaries in targeting New Zealand by providing best practice and world-leading information security services.

Detect indications of malicious activity or vulnerabilities, and provide timely and evidence-based advice to our customers on best practice techniques to mitigate potential risks to their operating environments.

Disrupt by preventing threats from harming our customers' environments by providing best practice mitigation advice and, when required, intervene to remove and dispose of these harmful threats.

- Significantly increased support provided to critical infrastructure and services organisations in the health, information technology and energy sectors.
- The model used to calculate the economic benefits of the NCSC's work has been updated to reflect newer studies about the harm caused by malicious cyber activity.

Since June 2016, the NCSC has reduced harm from hostile cyber activity by approximately $165.2 million.



Cyber defence

The NCSC's cyber defence capabilities, including CORTEX, provide New Zealand's nationally significant organisations with greater confidence in the security of their information and systems. This is crucial to business confidence and economic growth, and helps make New Zealanders safer and more prosperous in an increasing complex world economy affected by COVID-19.

The NCSC's cyber defence capabilities can be deployed at different points on a customer's network depending on their network configuration and risk profile. A key focus is countering advanced, persistent cyber threats which are typically beyond the detection and disruption capabilities of commercial products and vendors, and which might have a high impact at a national level.

The concept behind the NCSC's capabilities is more than just direct cyber threat detection and disruption. The NCSC provides incident response support to help nationally significant organisations address potentially high impact cyber events. If activity is targeting one customer's network, the NCSC can make the cyber threat information available to other customers. This enables organisations not directly protected by the NCSC, or that have not yet been targeted to identify and mitigate the threat, if needed. This is the premise behind the development of the NCSC's newest capability, Malware Free Networks.

The benefits of cyber defensive capabilities

The NCSC commissioned independent research in 2016 to establish the benefits to nationally significant organisations of its cyber defence capabilities in disrupting and preventing cyber harm.

The research focused on advanced cyber threats targeting nationally significant organisations which they were unlikely to be able to stop or detect themselves.

The intent to harm had to be highly targeted and have the potential to cause considerable harm to the integrity and availability of the systems, or the functioning and viability of the affected organisation. The types of harm considered were espionage and theft of intellectual property, inclusive of copyright and patent infringement.

The model has been updated in 2020 and continues to reflect respected international studies about the average costs of cyber harm across different sectors. This is translated into New Zealand equivalents, scaled for the number of organisations of potential interest, and factors in the complexity of each event.

Malware Free Networks

Malware Free Networks (MFN) is a scalable malware detection and disruption service which involves the NCSC generating and sharing cyber threat intelligence with consenting organisations. MFN is not a substitute for good cyber hygiene or commercial cyber security services but adds an additional layer to the cyber security of the NCSC's customers.

Cyber hygiene (or digital hygiene) is the routine practices and measures taken to minimise risks from cyber threats. Examples include maintaining system health and adhering to security measures.

In 2019/2020, the NCSC successfully piloted MFN and commenced the initial rollout of the service, through close collaboration with MFN Partners. Further development of MFN included engineering works such as solution design and implementation, and the development of operating procedures and standards. The NCSC also worked towards the Certification and Accreditation of MFN and supporting systems.

MFN is now being progressively rolled out to consenting NCSC customers, who will receive the MFN threat intelligence feed either directly from the NCSC or via MFN Partners, such as internet service providers or managed service providers. This approach ensures nationally significant organisations with varying capability levels are able to receive the benefits of MFN and will offer the NCSC's cyber security capabilities to a larger number of nationally significant organisations.

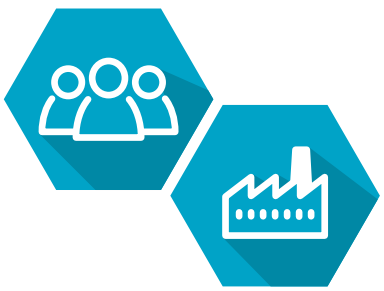
The delivery of MFN demonstrates the successful cooperation between public and private sector organisations and is an important part of the national strategy for increasing New Zealand's cyber resilience. The NCSC anticipates MFN will help analysts better understand the nature of threats targeting New Zealand organisations, and will inform the NCSC's wider cyber defence efforts.

Cyber resilience

The NCSC proactively engages New Zealand's government agencies and nationally significant organisations to improve their cyber resilience and inform them about emerging cyber threats. These organisations receive support, advice and cyber threat alerts from the NCSC, which helps to lift their overall cyber resilience and reduce their vulnerability to cyber threats.

Cyber resilience is a broader approach to security than just prevention; it also gives an organisation the ability to identify, respond to, and recover from cyber threats.

In 2019/20, the NCSC recorded 1,770 engagements with more than 250 organisations across a broad spectrum of public and private sector organisations. The NCSC also published 24 reports for general customers identifying specific vulnerabilities, providing mitigation advice, and reinforcing cyber security best practice to raise cyber resilience.



Over the year, the NCSC facilitated 20 regional and sector-based security information exchanges (SIEs). Bringing together information security professionals from government agencies and nationally significant organisations in the energy, finance, government, network, transport, logistics and education sectors. These exchanges allow participants to share information and enhance collaboration on cyber security challenges and opportunities across all sectors. SIEs generally meet quarterly and membership is restricted to nationally significant organisations.

In 2019, the 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.

The NCSC published guidance to help boards improve the cyber security governance of their organisations. The first in a series of resources to assist organisations in raising their cyber resilience, *Charting Your Course: Cyber Security Governance* is intended to support executive decision making related to cyber resilience and risk. This advice can be found on the NCSC's public website.

Government Chief Information Security Officer

Through the Director-General's role as the Government Chief Information Security Officer (GCISO), the GCSB takes a strategic approach to identifying security risk and working across government agencies to help enable effective responses. This includes identifying technical responses and making sure there are effective policy settings across government.

The NCSC contributes to this role by providing official advice to government agencies, which helps build and maintain a high level of cyber resilience and awareness among these agencies. The value of the NCSC's support was reinforced during the rapid shift to remote working at the onset of New Zealand's COVID-19 pandemic response.

Over 2019/20, advice was provided to government agencies, which was also made public, about security considerations when adopting alternative communications technologies. This enabled government agencies to conduct remote meetings over COVID-19 Alert Level 4, with an increased understanding of the relevant security risks and mitigations. The NCSC also provided security advice for pandemic tracking and contact tracing technologies being considered by government.

As the **Government Chief Information Security Officer**, the Director-General GCSB is the government functional lead for information security. This helps strengthen government decision making around information security and supports a system-wide uplift in security practice.

COVID-19

Like everyone else, the global COVID-19 pandemic and associated lockdowns impacted the way the NCSC operates. The NCSC very rapidly changed the way it works, to minimise the risk to staff and maintain continuity of essential services to New Zealand's nationally significant organisations.

During COVID-19 Alert Level 4 – Lockdown, the GCSB was deemed an essential service and as a result the NCSC focused on undertaking essential activity. Examples of this included maintaining detection and disruption services, providing guidance to government about maintaining safe and resilient digital services, and supporting essential networks within the national security sector.

The pandemic accelerated the pace of change and adoption of new technologies. The NCSC's customers undertook broad changes in their own work arrangements, as organisations in the public and private sectors sought to rapidly and securely adopt cloud platforms and systems for remote working. This included the adoption of internet-facing video teleconferencing solutions.

The NCSC saw increased demand for cyber security expertise and advice from existing and new customers. A range of cyber security advice and resources, including about remote working, were provided via the NCSC's public website and directly to customers, to encourage a high level of cyber resilience and awareness throughout the national pandemic response. During the early months of the pandemic response, the NCSC provided assessments and reports about international cyber security developments to a broader government readership.

Major events

In 2019/20, the NCSC commenced a programme of work to understand and mitigate cyber threats to major events. In other countries, major events have been linked to a wide range of malicious cyber activity by issue motivated groups, cyber criminals and state-sponsored cyber actors.

A key focus for the NCSC's major events work programme has been preparations for New Zealand's General Election in October 2020. Maintaining the integrity of the electoral process is a vital part of safeguarding New Zealand's democratic society. The NCSC is constantly considering threats and vulnerabilities, and works closely with international partners on their experiences with safeguarding elections.

In the lead up to the election, the GCSB and New Zealand Security Intelligence Service (NZSIS) reviewed and revised the protocol for suspected interference in the election, in consultation with the Electoral Commission. A similar protocol was in place for the General Election in 2017, but was never activated.

The NCSC directly supported the Electoral Commission to increase its cyber resilience, provided updated advice and assistance to political parties and candidates, and assisted with protective security briefings to Members of Parliament in conjunction with the NZSIS.

New Zealand's electoral process

The integrity of New Zealand's electoral process is at the heart of our democratic society and our elections must be free and fair. While the GCSB supports efforts to safeguard New Zealand's democratic process from interference by state actors, robust political debate and freedom of expression are fundamental to New Zealand's democratic process. The GCSB does not have any role in monitoring political discussion in New Zealand.

Updated terminology: allow list and deny list

The NCSC has adopted the use of the terms *allow list* and *deny list*, in place of *whitelist* and *blacklist*. This change has been made to promote a work environment where everyone feels valued and respected. It acknowledges the power words have in our society, and ensures the terminology used has clear and unambiguous meaning for the NCSC's customers.

This change in terminology is consistent with steps taken by the United Kingdom's National Cyber Security Centre, as well as many of the NCSC's other international partners. The NCSC encourages New Zealand organisations to adopt and normalise these new terms.

Privacy Act 2020

In June 2020, the New Zealand Parliament passed the *Privacy Act 2020*, which requires businesses that have suffered a serious data breach to notify the Privacy Commissioner and affected individuals. This law comes into force on 1 December 2020 and applies to all organisations that carry on business in New Zealand, regardless of where they are based.

This legislation will improve the New Zealand Government's understanding of the frequency and scale of data breaches that occur. Similar changes by Australia in 2018 saw an eight-fold increase in data breach notifications. This legislation comes as the personal information of New Zealanders is increasingly collected and stored digitally, and will improve the required standards for businesses holding personal information about New Zealanders, regardless of whether it is stored in New Zealand or abroad.

Who the NCSC works with

In order to effectively protect New Zealand and New Zealanders from advanced cyber threats, the NCSC works closely with 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 security incidents 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.

Internationally, the NCSC works closely with the Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the United Kingdom's National Cyber Security Centre, 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.

International landscape

Public and private sector organisations of all types and sizes are frequently affected by malicious cyber activity. According to cyber security researchers from Bromium, Cybersecurity Ventures and RiskIQ the cost to the global economy is at an all-time high. As society continues down the path of digital transformation many more devices are being connected to the internet each year, creating more opportunity for malicious cyber activity.

State-sponsored and criminal cyber actors target digital devices and networks using a continually evolving range of tools, techniques and procedures. They are quick to exploit new vulnerabilities, themes and digital behaviours, and aggressively exploit the digitalisation of the world economy for their own benefit.

The interconnected nature of the global cyber landscape necessitates an understanding of international trends and events, as emerging threats overseas can quickly impact New Zealand. To better defend New Zealand's nationally significant organisations from actors that may seek to harm them, the NCSC monitors emerging malicious cyber activity abroad and seeks to understand the context of the activities observed.

COVID-19: international impacts

Internationally, the global pandemic created many opportunities for malicious cyber actors to steal data, commit financial crimes, undertake espionage or disrupt the systems of organisations with a pandemic response role. Public fear, interest and desire for information was exploited through pandemic-themed lures and malware, which enabled malicious activity targeting specific organisations and the broader public alike. This activity matches normal patterns of behaviour for malicious cyber actors, who commonly modify their tactics to exploit current events.

Throughout the COVID-19 pandemic, cyber criminals demonstrated a disregard for threat to life and livelihood. Organisations involved in the crisis response were targeted by cyber criminals, who sought to impair the operation of hospitals, and other medical services and facilities. This reinforces the importance of good cyber security practices within any agency or organisation that may be involved in crisis management and the provision of services to the public, as cyber criminals quickly seek to exploit crises for their own financial benefit.

Sophisticated international cyber actors are taking advantage of the pandemic to carry out malicious cyber activity against systems and infrastructure central to the pandemic response in a number of countries. Throughout the global pandemic, the healthcare and pharmaceutical sectors are being targeted by malicious cyber actors, including state actors. State actors are also using malicious cyber activity to promote narratives about the origins of the virus and various countries' response to it.

The pandemic correlated with a significant increase of adversarial behaviour by malicious cyber actors. As lockdowns and border restrictions continue, states may increasingly rely on their cyber capabilities to undertake activities traditionally associated with other parts of their intelligence and security establishments. While the longer term impacts of COVID-19 on malicious cyber activity are unknown, there is potential for state actors to prioritise intellectual property theft or commercial espionage against academic and economic targets, to bolster their own national economies and pandemic responses.

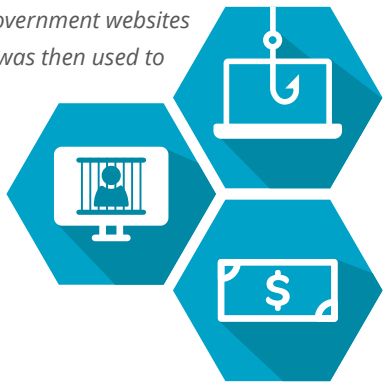
EXAMPLES OF MALICIOUS ACTIVITY ASSOCIATED WITH COVID-19

A very significant volume of COVID-19-themed phishing emails were sent by malicious cyber actors, who sought to steal user credentials, deliver malware or defraud individuals and organisations. Common lures purported to contain official information about the pandemic or financial aid relief.

The International Criminal Police (INTERPOL) issued an alert early into the global pandemic, to warn law enforcement agencies about international cyber criminals targeting the health sector. In some instances, ransomware operators specifically targeted organisations responding to COVID-19 outbreaks, including hospitals.

Cyber criminals exploited public anxiety in countries with high COVID-19 case numbers by distributing malware purporting to be smartphone applications for contact tracing or public information.

Cyber criminals defrauded COVID-19 financial aid funds of tens of millions of dollars. A typical example involved creating fake government websites to steal personal information from the public, which was then used to apply for financial aid.



COVID-19 contact tracing technologies

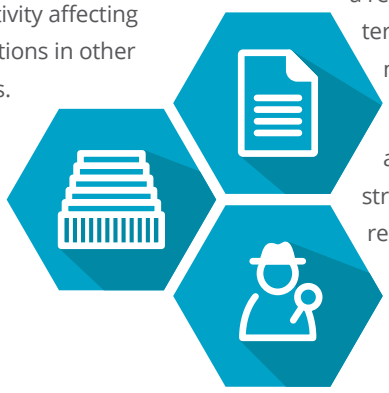
Countries are grappling with the challenge of providing contact tracing technologies, and simultaneously ensuring sensitive health data remains secure. While these technologies are not a silver bullet to managing pandemic outbreaks, they do give contact tracers a head start with identifying anyone who may have been exposed to COVID-19.

Any digital contact tracing solution comes with some risk. Their implementation requires a detailed consideration of cyber security risks, as malicious cyber actors regularly exploit new technologies. For example, malware disguised as contact tracing applications has been downloaded by users who download applications from outside of their phone's official storefront (e.g. Apple App Store or Google Play).

Upholding the rules-based order in cyberspace

New Zealand is committed to upholding the rules-based international order which contributes to the secure, resilient and prosperous online environment from which New Zealand benefits. New Zealand's Cyber Security Strategy highlights these values and asserts New Zealand's willingness to call out malicious cyber activity when it is in the national interest to do so.

GCSB continues to work closely with partner agencies across government and internationally to call out malicious cyber activity counter to internationally accepted norms of behaviour in cyberspace. On behalf of the New Zealand Government, in 2019/20 the Director-General of GCSB twice condemned malicious cyber activity affecting organisations in other countries.



In February 2020, GCSB's Director-General publicly condemned malicious cyber activity by Russian state-sponsored cyber actors targeting over 2,000 Georgian websites and the Georgian national television station in October 2019. This activity was designed to undermine Georgia's political processes and economic freedom. All states are urged to abide by the framework for responsible state behaviour online.

In May 2020, GCSB's Director-General publicly condemned international cyber actors taking advantage of the COVID-19 pandemic to carry out malicious cyber activity. This activity targeted systems and infrastructure central to the pandemic response in a number of countries. The targeting of such systems in any country, at any time, is unacceptable. It is contrary to the norms of responsible state behaviour and countries have a responsibility to ensure their territories are not knowingly used by malicious cyber actors.

Calling out malicious cyber activity in this way helps send a strong signal to the actors and states responsible that their conduct is unacceptable within the rules-based international order.

Data breaches

In 2019/20, data breaches involving personal information continued to feature prominently in the international cyber environment. Cyber criminals and other malicious cyber actors frequently adopt an industry agnostic approach to stealing sensitive data or personal information. Stolen data is commonly used to enable fraud, extortion or further malicious cyber activity.

Internationally, public and private sector organisations of all types and sizes were affected. Examples include electoral commissions, government agencies, political parties, financial services, airlines, healthcare providers, retail outlets, technology companies, accommodation providers, educational establishments and social networking services. New Zealand organisations were also not immune, with several serious data breaches being reported publicly during the year.

Data leaks are expected to become more widespread in frequency and scale. Personal information and other types of data is increasingly being centralised in online databases, which are being accessed by more people on a regular basis. There is considerable risk associated with poorly configured online databases, while cloud services and remote workers are becoming an increasingly common target for malicious cyber actors.

EXAMPLES OF DATA BREACHES

A Norwegian state-owned investment fund was defrauded of more than $10 million, following a data breach which revealed information about a forthcoming loan. The actors used this information to convincingly impersonate both parties to the loan.

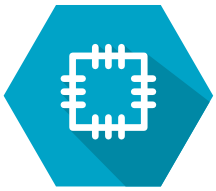
Smartphone applications used by election campaigns in multiple countries exposed the personal information of millions of voters. One instance saw personal information of millions of Israeli voters exposed. Another saw user credentials associated with a campaigning application stored in a publicly accessible database, which could have provided unauthorised access to personal information of millions of American voters.

Documents related to trade negotiations between the United Kingdom and United States of America were leaked online, and used in attempts to undermine the Government of the United Kingdom.

The personal information of almost the entire population of Ecuador was leaked online due to a misconfigured database. In some instances, the leaked data included familial, financial, employment and vehicle registration information.

Vulnerabilities

A **vulnerability** is a weakness which can be exploited by a malicious actor to perform unauthorised actions on a system. Vulnerabilities may exist in software, hardware, physical environments, organisational processes, personnel, or combinations thereof.



Malicious cyber actors continue to exploit known, unpatched vulnerabilities in networks, technologies and devices. Organisations should remain alert to newly publicised vulnerabilities in software, as good cyber security is dependent on organisations ensuring security updates and patches are applied as soon as they become available.

In 2019/20, malicious cyber actors sought to exploit a wide range of high and critical impact vulnerabilities in remote access and networking services. While attempts to exploit such vulnerabilities increased significantly as workplaces transitioned to remote work plans, they were observed throughout the year.

In one instance, Citrix disclosed a vulnerability which, if exploited, allows unauthenticated cyber actors to perform unauthorised actions. While mitigation advice and a security patch was made available, many organisations across the globe were compromised using this vulnerability. Similarly, publicly known vulnerabilities for Telerik UI and Pulse Secure VPN were widely exploited by a range of malicious cyber actors.

The exploitation of these vulnerabilities and the focus on remote access and networking services reinforces the importance of implementing good security practices. This includes adopting multi-factor authentication, strong password policies, regular reviews of network logs, and swiftly updating and patching services with publicly known vulnerabilities.

Ransomware

Globally, ransomware attacks occurred unabated through the year. Ransomware targeted every sector, including health and public sector organisations involved with pandemic responses. In many cases, organisations affected were multinational companies in the manufacturing and logistics sectors whose operations were affected globally.

Ransomware is a type of malicious software (malware) designed to deny access to a computer system or data until a ransom is paid.

While fewer incidents are occurring than the 2017/18 peak in ransomware activity, large organisations are increasingly affected in targeted, well planned incidents. Ransomware operators regularly target critical networks and services, to achieve the greatest disruption of business operations, and larger ransoms are being demanded than in previous years.

Ransomware operators are increasingly exfiltrating customer data or commercially sensitive information to increase their leverage in negotiations. Ransomware is now frequently the last step of an attack, deployed only after a malicious cyber actor has compromised and reconnoitred a device or network, exfiltrated data, and possibly destroyed or deleted backups. These types of ransomware incidents are also data breaches.

Paying a ransom may seem like a good option for an organisation to retrieve its data, but does not guarantee a swift return to normalcy. There are many ways a malicious cyber actor may respond after receiving a ransom payment and, assuming a ransom payment is honoured, negative consequences to paying remain. Payment enriches the criminal network, funds its ability to improve its techniques and validates the ransomware model. Researchers have also found paying a ransom usually increases the total remediation cost for a victim, as financial, labour, hardware and downtime costs are incurred while restoring systems, whether a ransom has been paid or not.

EXAMPLES OF RANSOMWARE

A range of municipal and state governments and agencies in the United States of America were the victims of ransomware. This affected schools, courts, law enforcement, payment systems, public communications and municipal services. In some instances, the severity of the ransomware incidents forced hospitals to cancel surgeries and inpatient services.

Australia's largest transportation and logistics company, Toll Group was the victim of two separate ransomware incidents. Both incidents affected the company's operational networks and customer-facing services for several weeks. The second incident was also associated with a data breach of employee details and commercial agreements. Cyber security researchers allege both incidents resulted from the exploitation of the same vulnerability.

One of the world's largest foreign exchange bureaus, Travelex, was the victim of ransomware. This affected operations in 26 countries for several weeks, and significantly diminished Travelex's ability to bear the financial costs of the COVID-19 pandemic.

Several European and North American companies in the electricity sector were victims of ransomware, affecting corporate and customer services. Electricity generation and distribution were unaffected in all reported incidents.

New Zealand landscape

New Zealand's nationally significant organisations continue to be frequently targeted by malicious cyber actors of all types. Throughout 2019/20, state-sponsored and non-state actors targeted public and private sector organisations to steal information, generate revenue, or disrupt networks and services .

Malicious cyber actors have shown their willingness to target New Zealand organisations in all sectors using a range of increasingly advanced tools and techniques. Newly disclosed vulnerabilities in products and services, alongside the adoption of new services and working arrangements, are rapidly exploited by state-sponsored actors and cyber criminals alike. A common theme this year, which emerged prior to the COVID-19 pandemic, was the exploitation of known vulnerabilities in internet-facing applications, including corporate security products, remote desktop services and virtual private network applications.

Organisations with poor security are more likely to become a victim of malicious cyber activity, and are much less likely to detect such activity before harm is caused. It is important organisations continue to adhere to strong cyber hygiene measures, such as regular patching and account audits, to ensure their systems are not susceptible to malicious exploitation.

Cyber security by consent

The NCSC works with organisations with their willing participation. Recognising this, the Intelligence and Security Act 2017 (ISA) does not require warrants for all activities. The NCSC is directly empowered to provide immediate assistance to organisations who have consented to receiving it, without the additional requirement of a warrant. This facilitates more effective and timely responses to potentially significant cyber incidents.

NCSC recorded cyber 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 domestic and international partners. NCSC incidents either involve organisations of national significance, or cyber threats that may affect New Zealand's national security and economic wellbeing.

During the 2019/20 financial year, the NCSC recorded 352 cyber incidents. Due to the NCSC's focus on nationally significant organisations, these incidents represent only a small fraction of the cyber security incidents that affected New Zealanders and New Zealand organisations.

For example, New Zealanders reported 5,653 incidents to CERT NZ over the year. Many compromises are also never detected or reported to New Zealand government agencies.

In a typical month, the NCSC's CORTEX capabilities detect 12 cyber intrusions affecting New Zealand organisations. In addition, the NCSC receives an average of 18 new incident reports per month, unrelated to CORTEX detection. These are typically self-reported by the impacted organisation or reported by the NCSC's partners.

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.

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

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

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

Compared to last year, incidents detected through CORTEX capabilities remained relatively steady, while more incidents are being reported unrelated to CORTEX detection. Self-reported cyber incidents continue to increase, possibly due to growing cyber security awareness and willingness to report incidents among New Zealand organisations. There was also an increase in notifications from the NCSC's international partners, demonstrating the highly transnational nature of the malicious cyber activity affecting New Zealand organisations.

The NCSC supports New Zealand victims of cyber incidents in several ways. Over 2019/20, the NCSC produced 82 reports for customers, alerting them to cyber security incidents or vulnerabilities affecting their networks. In some instances, this work included forensic investigations into compromises of New Zealand networks. In such cases, the NCSC worked with the New Zealand victim to assess the extent of the compromise, and provided detailed analysis and remediation advice.

COVID-19: domestic impacts

While cyber security researchers abroad reported a surge in COVID-19 related malicious cyber activity, the NCSC did not observe similar increases in malicious cyber activity affecting New Zealand organisations of national significance. In many international cases, an increase in pandemic-themed malicious cyber activity coincided with local and national outbreaks of COVID-19. New Zealand's relatively small number of COVID-19 cases and successful national response potentially reduced the opportunity for malicious cyber actors to exploit pandemic themes to target New Zealand organisations.

The pandemic has accelerated the adoption of technologies and greatly increased New Zealand's reliance on an open, secure and trusted cyberspace. The internet and digital technologies are central to continued economic activity during New Zealand's COVID-19 response, as well as the ability for various organisations to continue delivering services to the public. The increased adoption of digital platforms and solutions is expected to play a major role in improving business resilience, as well as promoting economic growth and business operations with the wider world.

Attack surface is the sum of all points where an actor can try to enter a system or extract data from. A network with many data interfaces has a larger potential attack surface to exploit than a network with a few carefully controlled access points.

Good cyber security postures and practices are increasingly important to safeguarding New Zealand's national security. The increased uptake and reliance on digital platforms by the private and public sectors increases the potential attack surface for malicious cyber actors, potentially increasing the likelihood and impact of a security breach.

Over the year, the NCSC published a range of advice on its website, which provides guidance to organisations adopting cloud services and remote work solutions. Cyber security risks should be considered by organisations undergoing digital transformation, and new services and technologies should be implemented with security configurations appropriate to their intended use.

State-sponsored linked incidents

New Zealand organisations remain the target of persistent malicious cyber activity linked to state-sponsored actors. During 2019/20, 30% of the NCSC's cyber incidents had links to state-sponsored actors. This is a smaller proportion than last year, as state-sponsored actors increasingly seek to obfuscate their malicious cyber activities by making it less distinguishable from both cyber crime and legitimate online activity.

State-sponsored cyber activity remains more sophisticated and persistent than criminal or non-state activity, and accounts for most of the NCSC's high priority cyber security incidents. This type of activity poses a more serious national security threat, as it is typically conducted for geopolitical or economic purposes and is more likely to affect organisations of national significance.

Direct and indirect cyber threats

New Zealand public and private sector organisations of all sizes and types face both direct and indirect cyber threats.

Direct threats have a specific and deliberate target that they are tailored to exploit. Potential targets include organisations in industries which hold information or insights of value to other states. This ranges from intellectual property and commercially sensitive information to customer data and government positions on sensitive topics. Organisations may also be deliberately targeted by those seeking to use their systems as malicious infrastructure against subsequent victims.

Indirect threats are less discriminate, and are typically delivered widely in hopes of compromising any vulnerable individual or organisation. Examples include the indiscriminate exploitation of publicly known vulnerabilities, targeting users of particular technologies, or targeting English-speaking countries more broadly. While indirect threats are typically less sophisticated, they can still cause harm to New Zealand organisations.

Detection of vulnerabilities

Malicious cyber actors regularly exploit publicly known vulnerabilities. The NCSC is aware that many malicious cyber actors use automated tools to conduct large-scale scanning to identify vulnerabilities or services being used on networks around the world. By identifying vulnerabilities at scale, malicious actors can prioritise their activity against those networks they are most likely to compromise. Additionally, by building a knowledge base of services being used on various networks, malicious cyber actors can quickly exploit newly disclosed vulnerabilities before security patches can be applied.

In 2019/20, 12% of reported cyber incidents were linked to known vulnerabilities in software and devices. In some instances, malicious cyber actors exploited vulnerabilities within weeks of their initial public disclosure. Several other vulnerabilities were publicly disclosed more than 12 months prior to their exploitation, highlighting the need for organisations to regularly patch their systems and conduct security testing to identify and mitigate known vulnerabilities.

Case study

The NCSC became aware a sophisticated cyber actor was targeting a sector in New Zealand that provided critical services to the public and held a significant amount of personally identifiable information.

The actor was assessed to be exploiting known website vulnerabilities which had been reported online though multiple sources over the past year. Once the vulnerabilities were exploited, the actor deployed malicious code onto the victim organisation's network to gain future access; allowing continued unauthorised access even after the vulnerabilities had been patched.

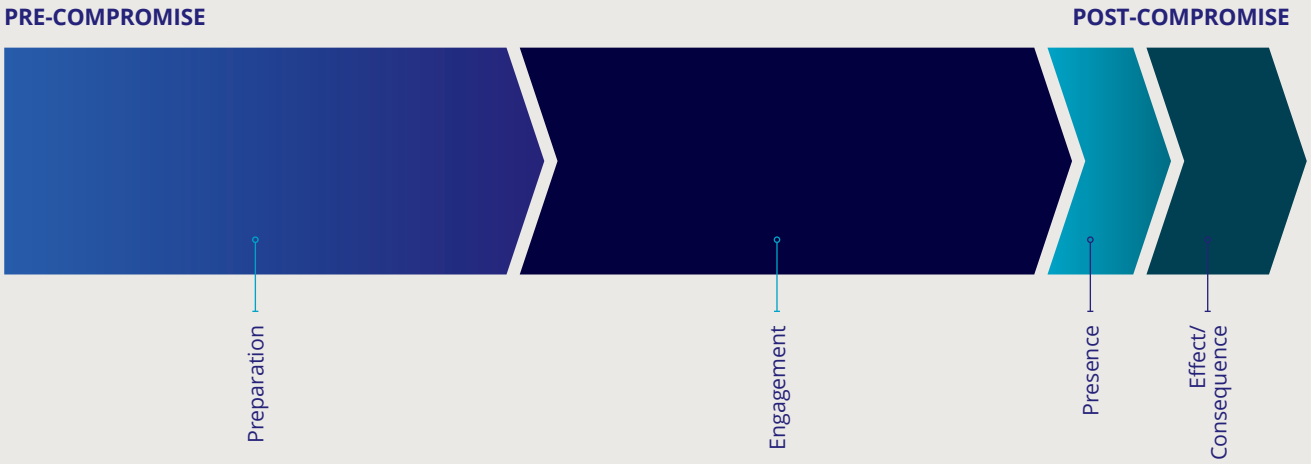
The NCSC undertook a proactive assessment to identify organisations whose websites were potentially vulnerable to this same activity. Once identified, the NCSC notified the organisations to recommend they patch the vulnerability and check for evidence of compromise within their networks.

Multiple organisations took action to secure their systems based on the NCSC's proactive assessment and advice.

In cases where known vulnerabilities are being exploited, the NCSC can provide mitigation advice directly to affected customers, potentially affected organisations or as security advisories on the NCSC website. On several occasions this year, the NCSC identified a vulnerability or incident impacting one customer, and provided relevant technical information to a wider set customers. Such notifications help New Zealand organisations detect potential incidents early, a critical factor in reducing the harm caused by malicious cyber actors.

Mitigating known vulnerabilities is crucial to safeguarding nationally significant networks and information from malicious cyber actors. In many cases, patching vulnerabilities after a malicious actor has already established persistence on a network or system will not remove the actor from the system. By advising customers about known vulnerabilities and indicators of malicious cyber activity, the initial compromise can be prevented.

Representation of incidents by phase



PRE-COMPROMISE INCIDENTS

Pre-compromise activity is characterised by planning and reconnaissance by cyber actors, or initial engagement with their targets. In 2019/20, 85% of the NCSC's recorded cyber incidents were identified before the point of network compromise. Pre-compromise incidents included brute force attempts, attempted code injections, denial of service activity, attempted malware deployment, phishing, reconnaissance, vulnerability scanning and website spoofing.

While pre-compromise incidents are lower on the range of severity, they may still have a significant impact on affected organisations. If not detected and mitigated in a timely manner, pre-compromise activity can evolve into fully fledged network compromise. Strengthening the first layer of cyber defence can have a significant impact in preventing a pre-compromise incident from escalating to a post-compromise cyber incident.

POST-COMPROMISE INCIDENTS

Post-compromise incidents are aimed at achieving ongoing access to a network, data exfiltration, or the disruption of networks and systems. In 2019/20, the NCSC recorded marginally fewer post-compromise incidents than last year, representing 15% of all cyber incidents. Post-compromise incidents included business email compromises, data exfiltration, internal network reconnaissance, malware deployment, and web server compromises.

Remediation of incidents that reach the post-compromise phase typically have significant impacts for the affected organisation, depending on the nature and extent of the compromise.

Cyber crime

The NCSC focuses on cyber incidents that are high impact and have national security implications, which includes some instances of cyber crime. In 2019/20, 14% of NCSC's cyber incidents contained indicators of criminal activity against public and private sector organisations. These included credential harvesting, data exfiltration, malware deployment, network and website compromises, and phishing.

The financial impact of cyber crime on affected organisations can be severe. Reputational impacts are also becoming more significant, particularly when cyber criminals exfiltrate and leak sensitive data or affect services to the public. Organisations can manage these risks by using a range of technical and internal controls, such as using multi-factor authentication and regularly patching known vulnerabilities.

While outside of the reporting period for this report, a global campaign of distributed denial of service (DDoS) activity in late 2020 affected a range of New Zealand organisations. This demonstrated the ability for less sophisticated malicious cyber activity to have a high national impact. While DDoS activity has been commonplace for more than 20 years, there has in recent years been an increase in the scale and complexity of DDoS activity. Organisations and their internet service providers are generally best placed to mitigate this risk.

Case study

The NCSC became aware of widespread exploitation of a known vulnerability in a network access gateway product used by many New Zealand organisations. When exploited, actors could obtain sensitive information or deploy malware, which could be used to gain access to the wider network.

The NCSC worked with organisations known to be using the network access gateway to determine the nature of any exploitation activity, provide remediation advice, and ensure the risk was mitigated.

Organisations who had implemented the vendor's mitigation advice before the public release of exploit code were protected from this activity.

Additionally, organisations who had well designed network segmentation in place were at lower risk of compromise from this activity, multi-factor authentication helped prevent unauthorised access, and restricting outbound internet access to authenticated users prevented the deployment of malware.

Case study

The NCSC engaged with an organisation whose web server was exhibiting behaviour indicating it was likely compromised. The NCSC worked with the organisation to identify the circumstances surrounding the compromise.

Forensic analysis identified an unpatched vulnerability in a popular content management system had been exploited on multiple occasions over a number of years.

These exploitation attempts facilitated the deployment of numerous web shells on the web server to maintain persistent access on the device. A web shell is a file, typically small in size, which allows a malicious actor to execute commands so long as it is present on the compromised machine.

Analysis identified sustained interactions with these web shells which included the creation of other malicious files as well as access to other resources containing credentials for other systems. The NCSC provided remediation advice to the affected organisation.

Conclusion

New Zealand receives many benefits from an open, safe and secure online environment. In an increasingly digital world, it is important for New Zealand that the online environment remains permissive to economic activity and secure for businesses and the public. New Zealand continues to support international efforts to maintain an open, safe and secure cyberspace .

This year, New Zealand's nationally significant organisations continued to be targeted by sophisticated state-sponsored cyber actors and cyber criminals alike. These actors quickly exploit new vulnerabilities, themes and digital behaviours, which increases the importance of resilient and responsive cyber security settings to defend New Zealand's critical systems and sensitive information.

Good cyber security promotes New Zealand's economic, social and cultural wellbeing, and in a physically isolated world New Zealanders need to have confidence in the security of their private, commercial, and nationally significant systems and information. New Zealand organisations – of all sizes and types – should get the basics of cyber security right, and give appropriate protection to New Zealand's systems and data.

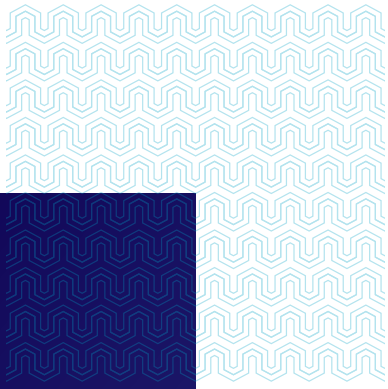
Organisations can take a range of straightforward, practical steps to increase their cyber resilience.

- Systems and applications should be regularly maintained, and patches or mitigations for newly disclosed vulnerabilities prioritised.
- Critical or sensitive data should be appropriately secured, especially when stored on cloud services or accessible from internet-facing servers.
- Systems and networks should be monitored for malicious or unusual activity, with effective logging implemented to aid detection of and response to such activity.
- Security should regularly be tested to identify vulnerable systems, services and processes before they can be exploited.
- Plans for responding to and managing cyber incidents should be established and tested.
- Cyber security training and practical guidance should be given to staff, including those who work remotely.

In combination, such actions create layers of cyber defence which makes it more difficult for malicious cyber actors to succeed, reduces the potential harm that may be caused, and enables an organisation to more swiftly detect, respond to, and recover from cyber incidents.

The NCSC supports New Zealand's continuing digital transformation by advising customers, deterring adversaries, and detecting and deterring malicious cyber activity which undermines the online environment. The NCSC remains committed to working with New Zealand's nationally significant organisations and partners across the public and private sectors to protect New Zealand's systems and data.

The consent and cooperation of the NCSC's customers and the public remains central to achieving the goal of creating a safer digital world for New Zealand to prosper. The NCSC hopes this report will promote increased cyber security and resilience, not just among the NCSC's customers but also across New Zealand organisations more broadly.



Getting in touch with us

If you have any questions related to this report, please contact the communications team at the GCSB.

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

Glossary

This glossary of terms 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.

TERM	DEFINITION
Advanced Persistent 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.
Credentials	A user's authentication information used to verify identity – typically a password, token or certificate.
Cyberspace	The global network of interdependent information technology infrastructures, telecommunication networks and computer processing systems in which online communication takes place.
Data Breach	The intentional or unintentional release of sensitive or private information into an unsecure environment.
Exfiltration	Where an actor has unauthorised access to private organisational data (for example, legitimate credentials or intellectual property), and removes it from a system.
Incident	An occurrence or activity that appears to have degraded the confidentiality, integrity or availability of a data system or network.

TERM	DEFINITION
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, such as viruses, Trojans or worms.
Mitigation	Steps that organisations and individuals can take to minimise and address cyber security risks.
Nationally Significant Organisations	Organisations such as government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.
Personal Information	Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI