NATIONAL CYBER SECURITY CENTRE

CYBER THREAT REPORT 2020/21

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

GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

CONTENTS

Ngā Kaupapa

FOREWORD

Whakapuakitanga

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau (GCSB). Our purpose is to create a safer digital world for Aotearoa New Zealand to prosper. We achieve this by supporting nationally significant organisations to protect their networks. The NCSC works to provide preventative advice on, and to deter, detect, and disrupt, the types of malicious cyber activity that could affect the country's national security or economic wellbeing.

The NCSC's annual Cyber Threat Report focuses on our analysis of incidents we have prevented, detected, or disrupted. It draws on and informs the wider functions and objectives the NCSC delivers on to lift the cyber security of nationally significant organisations.

In the 2020/21 year, the NCSC recorded 404 incidents with a possible national impact, or affecting Aotearoa New Zealand's nationally significant organisations. The increase in disruptive, criminally motivated activity among our incidents reflects the harm caused by ransomware and extortion campaigns. This activity increasingly targets critical service providers and organisations with no tolerance for extended periods of disruption. While less obviously disruptive, state-sponsored malicious cyber activity remains a focus for the NCSC, with 28% of recorded incidents showing links to suspected state-sponsored actors.

The NCSC welcomes increased public awareness about the seriousness the cyber threat poses to Aotearoa New Zealand and the work we do to counter it. Through our efforts to respond to incidents and reduce their impact, we provide significant benefits and cost-avoidance. In the 2020/21 year, NCSC intervention or advice prevented an estimated $119 million worth of harm to nationally significant organisations by either preventing incidents, or providing assistance and advice that helped those significant organisations detect, respond, and recover from malicious cyber activity. Since June 2016, this is an estimated total of $284 million.

The consent, ongoing co-operation, and collaborative approach of our customers and partners is critical to this success. By working together, the NCSC gains greater visibility and awareness about the types of serious malicious cyber activity affecting Aotearoa New Zealand's organisations. We use this information to strengthen everyone's defences. The NCSC's newest major defensive initiative, Malware Free Networks, will help us protect even more organisations by making our insights available through commercial partners.

A major part of our work is supporting organisations to increase their cyber resilience. The NCSC provides advice and guidance to network defenders and decision makers. In the 2020/21 year, the NCSC released publications about two of the biggest cyber security challenges facing Aotearoa New Zealand's organisations: supply chain security and incident readiness. The best-prepared organisations understand the value and importance of their information systems, have assessed their cyber security risks and dependencies, and are prepared to respond when incidents do happen.

Malicious cyber actors remain determined and well-resourced, and our nation's most significant organisations are not immune. I hope the NCSC's insights are valuable to anyone with an interest in Aotearoa New Zealand's security and wellbeing.

Lisa Fong (she/her)
Director, National Cyber Security Centre

BY THE NUMBERS

Mā ngā tau

IN THE 2020/21 YEAR THE NCSC AND GCSB

Received 141 notifications of network change proposals under The Telecommunications (Interception Capability and Security) Act 2013 (TICSA)

Conducted 29 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA)

Conducted 69 assessments under the Overseas Investment (Urgent Measures) Amendment Act 2020 (OIAA)

THE NCSC IN A TYPICAL MONTH

Detects 13 cyber intrusions affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities

Receives 21 new incident reports or requests for assistance unrelated to the NCSC cyber defence capabilities.

404

incidents affecting nationally significant organisations

A 15% INCREASE FROM THE 352 INCIDENTS RECORDED IN 2019/20

113

of those, or 28%, indicated links to suspected state-sponsored actors

COMPARED TO 30% IN THE 2019/20 YEAR

110

incidents, or 27%, were likely criminal or financially motivated

$119m

In 2020/21 the NCSC prevented an estimated $119 million worth of harm to Aotearoa New Zealand's nationally significant organisations

A TOTAL OF $284 MILLION SINCE JUNE 2016

2000

The NCSC disrupted over 2000 malicious cyber events as part of the early phase of Malware Free Networks

THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE

Recorded 1872 engagements with customers

Co-chaired 22 sector-based Security Information Exchanges

Published 23 reports and advisories for general customers

Delivered 94 incident reports to customers

OVERVIEW

Tirohanga Whānui

The Cyber Threat Report 2020/21 provides an overview of the NCSC's work during the year 1 July 2020 to 30 June 2021. It aims to highlight trends and observations about the nature of cyber incidents affecting Aotearoa New Zealand's organisations. The report also provides a review of the international cyber threat landscape and the context it sets for Aotearoa New Zealand.

The report first outlines the NCSC's mission, and describes the services the NCSC offers to Aotearoa New Zealand's nationally significant organisations. Much of the work carried out in the 2020/21 year focused on supporting these organisations to strengthen their awareness and resilience, and prepare for threats to their networks and information systems. The work programme involved significant new service provider partnerships to address security in digital supply chains. The NCSC also has a role in assisting the government to ensure the secure delivery of major events such as the General Election, the COVID-19 vaccination rollout, and digital hosting of the Asia-Pacific Economic Cooperation (APEC) forum.

In the 2020/21 year, the NCSC recorded 404 incidents – an increase of 15% on incidents recorded in 2019/20. A section dedicated to the Aotearoa New Zealand cyber threat landscape provides insights about these incidents. This section also describes how the NCSC defines an incident, and how severity ratings are assigned using an incident categorisation matrix. The year's three most severe incidents were rated category 2 or 'C2' – highly significant incidents. These comprise the Waikato District Health Board ransomware incident; a series of distributed denial of service incidents targeting Aotearoa New Zealand's stock exchange; and a data breach affecting the Reserve Bank of New Zealand. All three attracted significant media attention. A number of other case studies illustrate the range of incidents the NCSC handles.

Of the 404 incidents recorded, 28% showed links to suspected state-sponsored cyber actors. While the proportion of incidents showing connections to state-sponsored actors has reduced relative to previous years, this still amounts to 113 incidents. A further 27% indicated suspected criminal or financially motivated activity. The remaining incidents either had insufficient information to make any assessment about the type of actor responsible, or represented proactive, preventative efforts undertaken by the NCSC. These incidents reflect the difficulty of attributing activity to a particular actor, and the NCSC's focus on engaging early. The NCSC often prevents compromises long before it is possible to assess anything about the actor responsible or their motivation.

Malicious cyber activity in Aotearoa New Zealand largely matches international trends, with both ransomware and rapid exploitation of internet-facing services and applications a common trend in the 2020/21 year. A review of the international context, and some of the global issues attracting political and media attention, provides the final substantive section of this report. For readers unfamiliar with any of the terms used, or how the NCSC defines them, a glossary is provided after the report's conclusion.

ABOUT OUR WORK

Mō ā mātou mahi

The NCSC's purpose is to create a safer digital world so Aotearoa New Zealand can prosper. The information security services we provide support the protection, wellbeing, and prosperity of Aotearoa New Zealand.

Our focus is on assisting nationally significant organisations to lift their information security posture, with customers including government agencies, critical national infrastructure providers, major economic generators and intellectual property generators. We increasingly work with suppliers to nationally significant organisations, and we are available to assist whenever a cyber incident has the potential to cause serious harm or disrupt the country's security and economic wellbeing. High-impact security incidents have economic and social consequences that can have a lasting effect.

Our strategic objectives

- Defend National Security
- Raise Cyber Resilience
- Facilitate Digital Transformation
- Support Economic Recovery
- Improve Aotearoa New Zealand's Wellbeing

What the NCSC does

As the lead organisation for responding to cyber threats that could have an impact on national security and wellbeing, the NCSC works to reduce the chances that a significant cyber incident will happen in Aotearoa New Zealand. When incidents do happen, the NCSC takes action to reduce the impact and prevent future harm. To meet our strategic objectives we act in four ways: advise, deter, detect, and disrupt.

Advising means understanding the threat environment and preparing our customers for what might happen through a range of resilience-building services and advisories. This work also involves securing national supply chains through regulatory security risk assessments.

Deterrence discourages malicious cyber actors from targeting Aotearoa New Zealand by making it harder for them to operate here. Deterrence can range from protecting the government's most sensitive information, to publicly attributing malicious activity.

The NCSC's cyber defensive technologies and services find and share indications of malicious cyber activity by *detecting* anomalies and signs of compromise on consenting customer networks. The NCSC *disrupts* malicious cyber activity by sharing threat information across our customer base, intervening when a threat is detected, blocking specific threats to customer networks, and deploying our incident response team if necessary. The NCSC's incident responders help organisations evict malicious cyber actors from their networks, restore services, and recover.

Building resilience

The NCSC helps organisations understand their cyber security risk and provides guidance about how to manage it. By proactively engaging with organisations from a range of sectors, the NCSC aims to increase Aotearoa New Zealand's cyber resilience.

In the 2020/21 year, the NCSC released two publications for business leaders and cyber security professionals: *Supply Chain Security: In Safe Hands* and *Incident Management: Be Resilient, Be Prepared.* They are part of a series created by analysing 250 Aotearoa New Zealand organisations for the biggest cyber security challenges facing NCSC customers.

What's the harm?

In 2020/21, detection and disruption activities undertaken by the NCSC prevented an estimated $119 million of harm to New Zealand's organisations of national significance. This figure reflects incidents where NCSC engagements protected nationally significant networks from imminent threats that had the capacity to cause serious harm, or where our response prevented or reduced the harm caused by sophisticated and targeted attempts to compromise customer organisations. The increase from 2019/20's $70 million dollar harm reduction calculation reflects the increase in recorded incidents, as well as the scope of the NCSC's assistance to victims, and the critical economic roles and services provided by many of the victims affected by 2020/21 incidents.

In 2016, the NCSC commissioned independent research to devise a model that could measure the benefits provided by our interventions. The model was reviewed and updated in 2020 to ensure it better reflects international studies about the average cost of cyber incidents to specific sectors. It factors in important impacts, such as losses caused by intellectual property theft, including copyright and patent infringement. While assigning a dollar value to harm prevention can provide a useful benchmark, many of the impacts of cyber harm are intangible. Loss of public confidence and trust, reduced health and wellbeing, and hesitance to adopt new technologies can all eventuate when cyber resilience is low.

In 2020/21, the NCSC recorded 1872 engagements with 200 organisations, and published a range of security advisories about threats to Aotearoa New Zealand organisations. Security advisories for general customers share information about specific vulnerabilities or types of malicious cyber activity seen targeting Aotearoa New Zealand networks. They may incorporate technical indicators and mitigation advice that security teams can use to strengthen their defences.

Threat information and best practice guidance are also generated by public and private organisations and the information security industry. The NCSC assists the facilitation of information sharing among organisations facing similar threats and challenges – especially where sharing requires a high level of trust. This primarily happens through Security Information Exchanges (SIEs) focused on critical infrastructure. In 2020/21, the NCSC co-chaired 22 SIEs. Participants include key organisations in the energy, finance, network-provider, government, transport and logistics, and tertiary education sectors.

Support to major events

Planning for major national events involves preparing for the possibility that a cyber security incident could cause disruption and reputational harm. The NCSC has a framework in place for supporting the cyber security requirement of major events. This involves proactively evaluating and preparing for cyber threats from state-sponsored actors, issue-motivated groups, and criminals.

In 2020/21, three significant events drew NCSC involvement. In addition to supporting the COVID-19 vaccine rollout, the NCSC provided services and advice to ensure the October 2020 General Election was free from cyber interference. Free and fair elections are integral to our democracy. While the GCSB does not have any role in monitoring political discussion or free speech in Aotearoa New Zealand, it is alert to the fact that foreign interference is a growing threat globally and domestically. The NCSC worked with the Electoral Commission to help protect its core systems and online presence. The NCSC also worked alongside relevant agencies to provide protective security and cyber security advice to political parties and candidates in the lead-up to the election.

Between November 2020 and November 2021, Aotearoa New Zealand hosted the virtual APEC 2021 forum. The NCSC assisted agencies involved to ensure the virtual hosting platforms used to facilitate online meetings were secure, and that risk assessment and mitigation processes were in place to protect participants. By successfully adapting to hosting APEC virtually, Aotearoa New Zealand played a leadership role in championing the APEC goal of building an open, dynamic, resilient, and peaceful Asia-Pacific community.

Ransomware is a type of malicious software (malware) designed to disrupt the use of computer systems and files until a ransom is paid. Crypto malware is a specific form of ransomware that encrypts files and requires a key – usually held for ransom by the malicious cyber actor – to reverse the encryption.

Supporting the COVID-19 vaccine rollout

As part of Aotearoa New Zealand's response to COVID-19, the NCSC extended support and advice to healthcare, logistics, transport, and IT system suppliers involved in all aspects of the national vaccine rollout. The NCSC identified points in the vaccine supply chain that could be vulnerable to malicious cyber activity. This information fed into national risk management planning.

In May 2021, the Waikato District Health Board (DHB) experienced a ransomware incident. The NCSC publicly acknowledged involvement in the DHB's recovery efforts. The reasons for the NCSC's participation were twofold: first, the NCSC was ready to respond to any malicious cyber activity that had the capacity to disrupt the country's COVID-19 response. Second, the incident degraded healthcare services and represented a threat to people's safety and wellbeing. Part of the NCSC's role was to support the DHB in safely restoring services. The NCSC also co-ordinated a wider defensive response, working to share information, and manage cyber security risk to the rest of Aotearoa New Zealand's healthcare sector.

Who the NCSC works with

The NCSC works with a number of partner organisations to build a cohesive line of cyber defence. Our primary international relationships are with the cyber security components of the Australian Signals Directorate (ASD), the Canadian Security Establishment (CSE), the United Kingdom's Government Communications Headquarters (GCHQ) and the National Security Agency in the United States (NSA). Respectively, their cyber security components include the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the United Kingdom's National Cyber Security Centre (UK NCSC) and NSA Cybersecurity.

Aotearoa New Zealand's Cyber Security Emergency Response Plan (CSERP) sets the framework for the government's response to a cyber security emergency, and prescribes the NCSC as the lead agency in Aotearoa New Zealand for incidents categorised as cyber emergencies. The NCSC works with CERT NZ, which provides general support to businesses, organisations, and individuals affected by cyber security incidents, and with New Zealand Police, which is responsible for investigating crimes that happen online.

Cyber security resilience is centrally important to ordinary business operations. The NCSC works closely with technology and investment advisors, including the Ministry of Business, Innovation and Employment (MBIE) and the Overseas Investment Office.

The NCSC values key partnerships with the private sector. During incidents, the NCSC typically works with suppliers to the affected organisations during the secure restoration of services. The NCSC is partnering with service providers to deliver more security offerings and enhanced security capabilities.

At a broader scale, the NCSC supports the government's wider digital and data goals in support of the nation's economic recovery and Aotearoa New Zealand's wellbeing. This work includes contributing to some key strategies: the Digital Strategy for Aotearoa, the Strategy for a Digital Public Service, the Data Investment Plan and the National Cyber Security Strategy, led by colleagues in the Department of Internal Affairs, MBIE, Statistics New Zealand and the National Cyber Policy Office.

Cloud security

As part of the GCISO's role to build and maintain a high level of cyber resilience and awareness in the public sector, in 2020/21 the NCSC began building NZISM baseline cloud security templates. These templates, developed in partnership with cloud service providers, better enable government agencies which are adopting cloud services to identify how their security controls and principles can be brought in line with best practice standards outlined in the NZISM. By using these templates, organisations will better understand their environments' level of compliance with relevant principles and controls, and be able to easily implement and continuously monitor their cloud services use to ensure they are maintaining a base level of protection.

The Government Chief Information Security Officer (GCISO)

The Director-General of the GCSB holds the role of the Government Chief Information Security Officer (GCISO), and is responsible for providing leadership and advice about information security risks across the public sector. The GCISO function draws on the technical capabilities of information security professionals from the GCSB, particularly the NCSC. Leveraging this expertise, the GCISO identifies solutions to common security challenges, ensures effective policy settings are in place across the public sector, and supports national incident response efforts.

The GCISO's efforts are also focused towards supporting the secure digital transformation of the public service. The GCISO uses specialised knowledge of international best practice and Aotearoa New Zealand's cyber threat landscape to help inform the information security standards for the public sector so they are appropriate, responsive, and relevant. GCISO develops and maintains the New Zealand Information Security Manual (NZISM), enabling digital transformation by setting high standards for information technology and communication systems. As the keystone information security policy-setting organisation, GCISO works closely with the functional leads including the Government Chief Digital Office (Department of Internal Affairs), Government Chief Data Steward (Statistics New Zealand) and the Government Protective Security Lead (New Zealand Security Intelligence Service (NZSIS)).

Cloud Services provide convenient, on-demand network access to shared pools of computing resources (such as servers, storage, and applications).

Regulatory functions

Aotearoa New Zealand's telecommunications networks are a core part of New Zealand's critical national infrastructure. Organisations and individuals rely on network providers for safe and secure access to digital capabilities, and the secure provision of telecommunications services.

The purpose of the Telecommunications (Interception Capability and Security) Act 2013 (TICSA) in relation to network security is to prevent, mitigate, or remove security risks arising from the design, build, and operation of public telecommunications networks, or from the interconnection of public telecommunications networks to networks in Aotearoa New Zealand or overseas.

Part 3 of TICSA establishes a framework under which telecommunications network operators are required to engage with the GCSB, via the NCSC, about network changes or developments that intersect with national security. Many of these changes are currently driven by cloud adoption, increased demand for remote working, the rollout and expanded capacity of fibre optic cabling, and the transition to 5G services. In the 2020/21 year, the GCSB received 141 notifications for assessment of network changes. A significant number of these related to the rollout of 5G and full-fibre networks.

The GCSB's other regulatory mandates are derived from the Outer Space and High-altitude Activities Act 2017 (OSHAA), and the Overseas Investment (Urgent Measures) Amendment Act 2020 (OIAA). Under OSHAA, NCSC and GCSB assist NZSIS and other agencies in assessing space and high altitude activities for national security risks. In the 2020/21 year, the GCSB conducted 29 assessments of regulated space activities. The GCSB's growing regulatory role also includes supporting the NZSIS to provide advice to the Overseas Investment Office about any national security risks associated with proposed overseas investment; in 2020/21 the NCSC conducted 69 assessments under the emergency notifications regime of the OIAA.

Privacy Act 2020

On 1 December 2020, Aotearoa New Zealand's new *Privacy Act 2020* came into force. Organisations that carry out business in Aotearoa New Zealand are bound by the Act regardless of where they are based. The law requires organisations that suffer a significant breach that either has caused or is likely to cause anyone serious harm to report that incident to the Privacy Commissioner.

While not every breach of privacy is the result of a cyber security incident, many organisations affected by cyber security incidents will need to report privacy breaches. When high impact incidents prompt the NCSC's assistance, incident responders can provide the forensic support and expertise required to identify whether personal information has likely been leaked or stolen, and to what extent. This helps organisations understand the potential harm a breach could cause and advise those affected.

Personal Information is information about an identifiable individual. The purpose of the Privacy Act 2020 is to promote and protect individual privacy.

Cyber defence

Aotearoa New Zealand's reputation as a place to invest, innovate, and embrace technology needs a cyber security culture that people respect and trust. The NCSC builds collaborative relationships with our customers, and offers defensive tools and capabilities to consenting organisations that choose to consume them. Increasingly, the NCSC is seeking out innovative ways to provide threat information to organisations involved in supplying IT or network services to New Zealanders.

The NCSC can deploy defensive capabilities, including those developed through the CORTEX project, to participating nationally significant organisations. These services are tailored to meet the network configuration and risk profile of each organisation. The NCSC's defences aim to keep customers ahead of sophisticated, advanced persistent threats. If malicious cyber activity is detected on one customer's network, the NCSC can derive threat information from the incident and use it to mitigate the threat to other customers. The principle of sharing information to strengthen everyone's defences underpins the NCSC's next major initiative: Malware Free Networks.

Malware Free Networks

Malware Free Networks (MFN) is a malware detection and disruption capability that will empower the NCSC to scale up our network protection services and block malicious cyber activity before it affects Aotearoa New Zealand organisations. The goal is to disrupt sophisticated malicious cyber activity as early as possible, for as many networks as possible. Through MFN, the NCSC generates and shares cyber threat intelligence with participating organisations. Customers can receive the MFN threat intelligence feed via MFN partners, such as internet or managed service providers.

In 2019/2020, the NCSC successfully commenced the initial rollout of the live service, which has been operating for a small number of consenting NCSC customers since August 2020. By July 2021, MFN had already disrupted over 2000 malicious indicators before they had the chance to cause harm. The NCSC aims to scale the availability of MFN through growing partnerships; the intention is to partner with industry organisations – from large telecommunication providers, to mid-sized managed service providers and small technology integrators – to make the MFN service available to as many organisations as possible. The NCSC anticipates MFN will grow to block more malicious traffic over time, and will provide unique threat insights and intelligence in support of increased detection.

Incident response services

When an incident does happen, the NCSC's 24/7 incident coordination and response team assists organisations to respond and recover. The team can draw on all the NCSC's resources to support and coordinate response efforts. If necessary, the NCSC's incident responders are deployed on-site, working side-by-side with victim organisations and their service providers as they recover. The NCSC provides forensic analysis and investigation capabilities to map the pathways a malicious cyber actor has taken, and evaluate the extent and impact of an intrusion. The NCSC can also provide advice and guidance on managing communications and keeping stakeholders informed during an incident.

In 2020/21, the GCSB publicly disclosed the NCSC's involvement in three high-profile incidents. These included assisting the Reserve Bank of New Zealand following a data breach, providing support to the Waikato District Health Board following a ransomware incident, and advising NZX with respect to a series of distributed denial of service incidents targeting Aotearoa New Zealand's stock exchange. All three of these incidents were rated as C2 incidents, or highly significant, and all attracted well-warranted public concern. Generally, to protect relationships of confidence and trust, the NCSC does not comment publicly on incidents or victims of malicious cyber activity.

A **Denial of Service (DoS)** incident is an attempt to make an online service unavailable by overwhelming the service with more traffic than it can handle.

AOTEAROA NEW ZEALAND THREAT LANDSCAPE

Te āhuatanga o ngā tuma i Aotearoa

While major disruptive incidents like denial of service and ransomware incidents dominated cyber news headlines in 2020/21, Aotearoa New Zealand's nationally significant organisations faced a broad range of cyber threats, including espionage and information theft.

Aotearoa New Zealand has a relative level of wealth, high digital interconnectivity, and niche technology exports. These factors contribute to the attractiveness of Aotearoa New Zealand as a target for motivated, well-resourced malicious cyber actors. Malicious cyber actors of varying levels of sophistication and motivation target Aotearoa New Zealand networks and create new and fast-moving challenges for network defenders. The NCSC's focus is on assisting customers through early warnings, prevention, harm reduction, and prompt service recovery.

2020/21 NCSC incidents

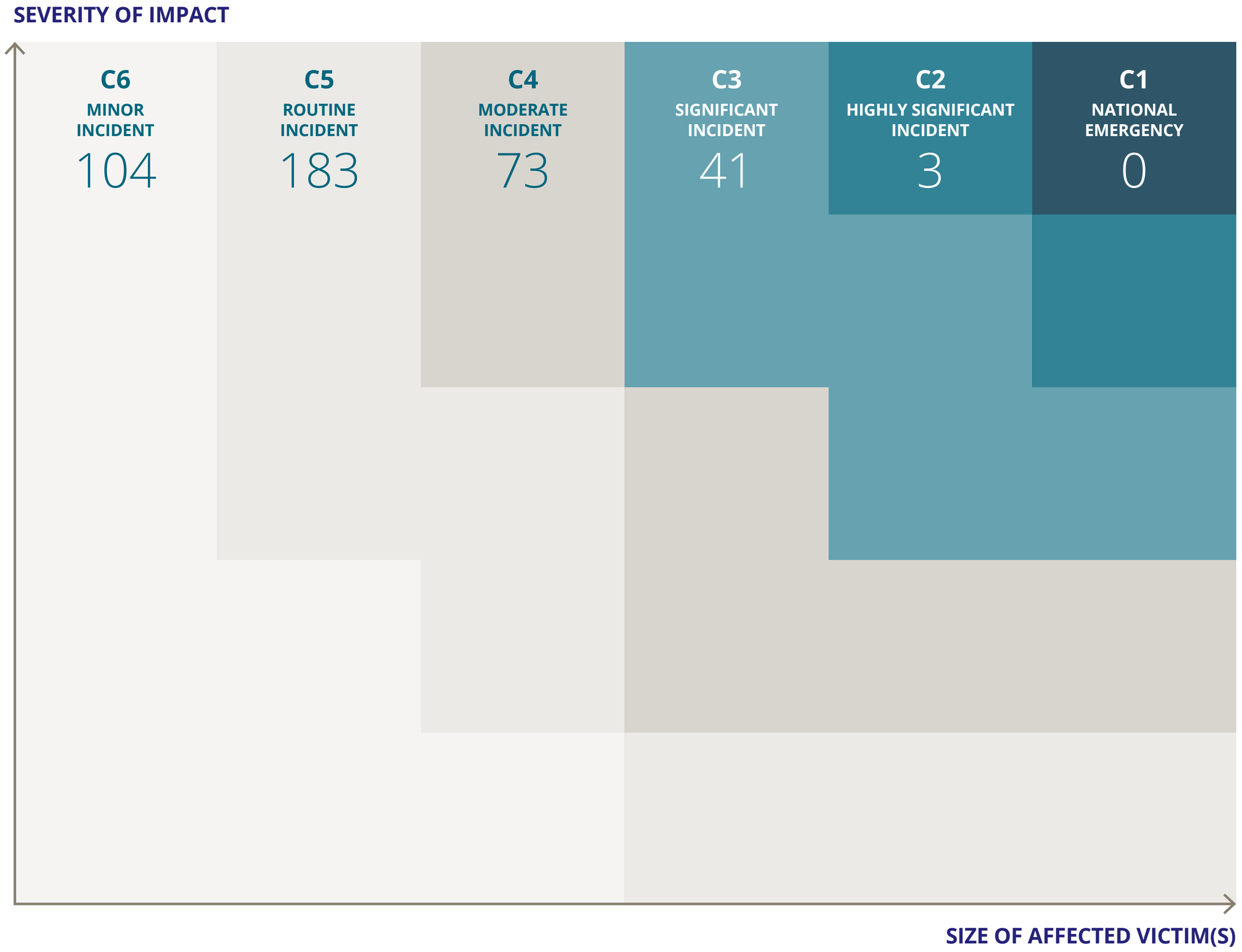
In the 2020/21 year, the NCSC recorded 404 cyber incidents. Because of the NCSC's focus on defending nationally significant organisations, this number represents a small but impactful portion of all cyber security incidents affecting Aotearoa New Zealand.

The incidents recorded by the NCSC come from a range of sources. These incidents are also a proportion of malicious cyber incidents affecting these organisations. Some are generated through reports or requests for assistance received from victims; some are reported to the NCSC by domestic and international partner agencies; a number are detected through the NCSC's cyber defence capabilities. Over the course of an average month in 2020/21, the NCSC handled 33 incidents. Of those, typically, 13 were detected through the NCSC's own capabilities. The remaining 21 were either self-reported or triggered by a domestic or international partner alerting us to the possibility of an incident.

How the NCSC defines incidents

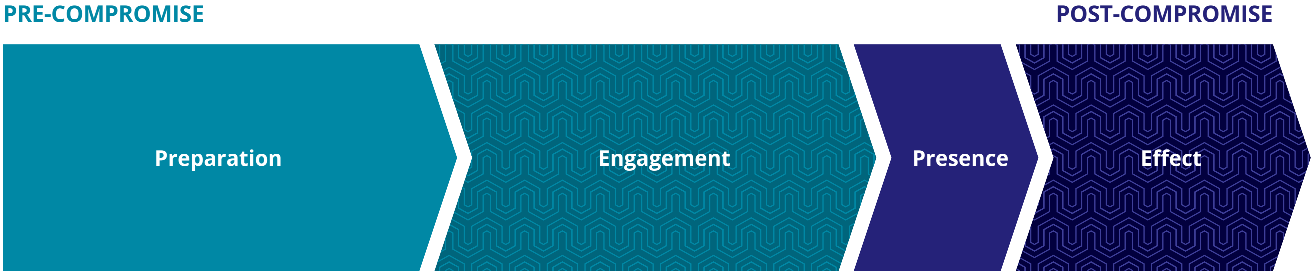
An incident can be any threat to a customer's network or information, even where an actor is unsuccessful or there is no confirmed compromise. Reconnaissance and network scanning, possible attempts to exploit customer vulnerabilities, accidental data leaks, or suspicious events that trigger analysis to determine if they are malicious might all be counted among the NCSC's total incidents.

The NCSC categorises incidents by considering the scope, size, and role of the affected victim alongside the possible harm and impact caused by the incident. Incidents range from category 6, being minor or of least concern, to category 1, being critical.



CATEGORY/DESCRIPTION	COUNT
C1 National Emergency	0
C2 Highly Significant Incident	3
C3 Significant Incident	41
C4 Moderate Incident	73
C5 Routine Incident	183
C6 Minor Incident	104

Highly significant incidents (C2) consume a substantial measure of time and resources, but even significant (C3) or moderate incidents (C4) can take a number of weeks to resolve, and will generally involve complex responses across a number of teams. For minor or routine incidents (C5 or C6), the NCSC might respond by providing general advice or alerts to customers. During the 2020/21 year, the NCSC delivered 94 cyber security incident reports or incident analysis reports to specific customers, and provided 23 general advisories or guides.



Malicious incidents by phase

For malicious cyber incidents and network compromises where an actor is involved, the NCSC records how far along an actor has progressed through the typical phases of a cyber incident – with activity spanning from initial staging, reconnaissance, scanning, networking profiling, and delivery of phishing emails – through to sustained network access or service disruption.

PRE-COMPROMISE INCIDENTS

In the 2020/21 year, 67% of malicious cyber incidents reached pre-compromise phases. Typical pre-compromise incidents involved network scanning, delivery of phishing emails, attempted but unsuccessful denial of service activity, attempts to brute force usernames and passwords, and unsuccessful attempts to exploit vulnerable software.

POST-COMPROMISE INCIDENTS

Post-compromise incidents include those where a malicious cyber actor has gained network access, succeeded in moving laterally through a network, or achieved an effect that denies, disrupts, degrades, or destroys the victim's information or system accesses. In the 2020/21 year, 33% of malicious incidents fell into the post-compromise category. This a significant increase from the 2019/20 year, when just 15% of incidents fell into this category. A large proportion of these were denial of service or ransomware incidents. While a ransomware incident can happen quickly, there is usually a window of time to detect and evict intruders before they are able to execute a full compromise. By contrast, a denial of service incident happens with almost no warning, and immediately falls into the final stage of having an effect on the victim. Denial of service attacks require long-term business continuity planning and early preparation to avoid suffering their full impact.

Links to state-sponsored actors

In the 2020/21 year, 28% of the NCSC's 404 recorded incidents showed indications of a connection to state-sponsored actors. The slight reduction in this proportion relative to previous years likely reflects an increase in the proportion of criminal or financially motivated incidents recorded. The number still totals 113 incidents of concern.

State-sponsored cyber activity is less likely to disrupt services or cause obvious harm, and less likely to enter the public spotlight, but the impacts for Aotearoa New Zealand's economy and effective international presence are very real. Sophisticated, state-sponsored actors aim to hide their intrusions while extracting valuable data from both public and private sector organisations. Successful actors steal information to gain geostrategic and political advantage, and to maintain pace with developments in scientific and technological research.

Financially motivated or criminal activity

An important trend in the 2020/21 incidents is the prominence of criminally motivated activity with a significant national impact or potential to cause serious harm. Of the NCSC's recorded incidents, 27% showed indications of suspected criminal or financially motivated actors (in comparison to 14% last year). This number reflects increased reports of disruptive ransomware and denial of service incidents against Aotearoa New Zealand's nationally significant organisations. These actors aim to apply pressure and extort payments from high-value, high-reward victims by deliberately disrupting critical services.

Criminal or financially motivated cyber actors increasingly share resources, and outsource parts of their work (such as developing new malware or acquiring infrastructure) to other groups. Shared common tools and infrastructure, along with the growing sophistication and resourcing of criminal actors, make it increasingly hard for the NCSC to distinguish between state-sponsored and non-state actors. This is especially true for incidents where the NCSC intervenes early. Intervening early reduces the chance that strong links to an actor or clear signs of motivation are detected and analysed.

Attributing malicious activity to a particular state is complex. The growth in the marketplace for sale and exchange of services, tools, and malware will continue to add to this complexity. Criminally motivated groups now have capabilities previously associated with well-resourced state actors, and some operate across jurisdictions or from locations that provide safe-havens or high levels of tolerance for their activity.

In the 2020/21 year, 26%, of incidents had insufficient information to make any assessment about the actor responsible or their motivation, and the suspected actor was recorded as unknown. The remaining share of incidents comprised proactive or preventative efforts, false positives, data leaks, or other incidents not associated with a suspected malicious actor.

Case study

The NCSC became aware of a sophisticated cyber actor targeting an Aotearoa New Zealand organisation that provides niche IT services internationally.

The NCSC worked with this organisation to identify the circumstances surrounding the compromise. Analysis identified the actor gained initial access by exploiting a vulnerability in a workstation hosted overseas and used this access to remotely connect to a workstation in Aotearoa New Zealand. Using a virtual private network (VPN) user account, the actor was able to move laterally and compromise administrative user accounts to gain further access into the network. The organisation was concerned the actor may have exfiltrated source code for one its core software products. The precision of this activity strongly suggested it was targeted at the organisation rather than being opportunistic.

Common Vulnerabilities and Exposures (CVEs)

The speed and indiscriminate nature of malicious cyber campaigns aimed at compromising common vulnerabilities continues to challenge Aotearoa New Zealand organisations. Many malicious cyber actors work rapidly to exploit new vulnerabilities in public-facing services and applications before organisations have time to prepare, test, and install security updates. Newly identified critical vulnerabilities are scanned for and exploited less than a week after they are announced, and sometimes within a day or two.

Incident data from the 2020/21 year reflects how the NCSC is responding; 16% of recorded incidents were associated with proactive, preventative effort. A large portion of these incidents involved identifying campaigns to exploit vulnerabilities, detecting those vulnerabilities on customer networks, and proactively notifying at-risk customers.

Many malicious cyber campaigns fully automate the process of scanning for vulnerabilities, conducting initial network breaches, and installing malware. These campaigns indiscriminately gain footholds on any vulnerable networks, with actors returning to select the highest-value targets from within a set of already-compromised networks. The speed of automated exploitation for newly announced vulnerabilities is now routinely faster than patching cycles, even for well-resourced organisations with good security practices. In addition to patching and maintaining software, organisations need to check for signs of a compromise in any situation where their network might have been vulnerable, even for a short window of time.

Organisations often underestimate the harm a cyber incident can have on their ability to maintain critical services and functions. Accurately anticipating and planning for how long it could take to recover from a compromise is an important part of understanding cyber risk, and allocating resources to manage it. The 2020/21 year illustrated the value good incident response and business continuity planning delivers. The best-prepared organisations adopted a 'not if, but when' approach to their cyber security.

Case study

The NCSC became aware of a ransomware incident impacting a research organisation.

The NCSC worked with this organisation to identify the circumstances surrounding the compromise. Analysis identified the malicious cyber actor initially gained access to the victim's network using valid user credentials. These credentials were likely obtained when a separate actor published a list of stolen usernames and passwords online; the stolen credentials were almost certainly sourced by exploiting a common firewall vulnerability. While the actor's ransom note claimed confidential data had been exfiltrated, NCSC analysis did not identify evidence of any data exfiltration.

The majority of the organisation's systems were taken offline as a result of the ransomware incident. The NCSC provided incident response services to identify the source of the compromise, determine what actions the actor undertook while on the network, and provide remediation and recovery advice.

Analysing trends in tactics and techniques

In 2020/21, the NCSC started using MITRE ATT&CK as a framework to map cyber security incidents. MITRE ATT&CK is a public knowledge base that provides a common set of terms to describe the tactics and techniques used by actors during various stages of an intrusion. By mapping recorded incidents to MITRE ATT&CK, the NCSC can gain insights into common or emerging trends in actor tactics and techniques.

Across malicious incidents from the 2020/21 year, the most commonly occurring technique was vulnerability scanning, and the most commonly recorded method of gaining initial access to a network was by exploiting a public-facing application.

While phishing remains common, many organisations have improved their defences and acquired security products that scan and manage email traffic well. Most computer users now have a sound understanding of how to identify and avoid malicious emails. In response, malicious cyber actors have found new ways to breach network perimeters and gain initial access to target networks; the new preferred method of access observed by the NCSC is exploiting software vulnerabilities.

Data theft

Both state-sponsored and criminal actors may steal valuable intellectual property to generate revenue or achieve a technological advantage. Proprietary software and other technology-driven products represent a growing industry in Aotearoa New Zealand, with significant growth in export sales in recent years, and a surge in investment and large acquisitions of Aotearoa New Zealand technology companies. To remain competitive and profitable, these companies need to protect their intellectual property from cyber-enabled theft.

Data theft is an increasingly common extortion tactic among cyber crime actors, with many ransomware actors stealing intellectual property or personal information from victims and threatening to reveal or on-sell this information unless a ransom is paid. The prevalence of this extortion tactic is likely to increase in future as criminal actors adapt their methods in response to defenders. While denial of service and ransomware incidents are costly, and present immediate business impacts, service recovery and remediation are always possible and many organisations plan for how to recover from these incidents. The harm caused by a data breach is much harder to remediate, especially where data represents an organisation's most valuable asset.

Case study

The NCSC detected malicious cyber activity affecting a public sector organisation in Aotearoa New Zealand. The NCSC alerted the victim organisation, and worked with their staff to identify the circumstances surrounding the compromise. Further investigation indicated the compromise had unfolded over a number of months, escalating as the actor explored the victim's network and began to understand its value.

NCSC analysis indicated the compromise probably began as an opportunistic effort to access a broad range of networks via automated exploitation of an unpatched vulnerability (CVE). The actor probably exploited a firewall to obtain credentials for several administrative user accounts, which later enabled them to connect remotely to the victim's network using the victim's own VPN. The actor then deployed malware on the victim's network and established ongoing remote access. The actor likely recognised the value in maintaining access to the victim's network in pursuit of valuable personal or commercially sensitive information. The NCSC assisted the victim to trace and contain the compromise, assess the impacts, and evict the actor.

INTERNATIONAL LANDSCAPE

Te āhuatanga i te ao

The extent and severity of malicious cyber activity conducted by both criminal and state-sponsored actors is attracting growing public and media attention. Globally, incidents and trends mapped closely to what the NCSC observed in Aotearoa New Zealand in 2020/21.

Organisations around the world felt the impact of high profile, sophisticated ransomware incidents that caused significant service disruption. Supply chain compromises and mass exploitation of vulnerabilities in popular software prompted concern and condemnation from industry professionals, public institutions, and governments. States increasingly see the impact of cyber security incidents, including ransomware and cyber crime, as a matter of national security. In response, political leaders have grown bolder in calling out activity that contravenes expected norms of acceptable behaviour in cyberspace.

Ransomware

The global prevalence of ransomware attracted considerable political and media attention in the 2020/21 year, with high-impact incidents affecting critical infrastructure both in Aotearoa New Zealand and abroad. Ransomware actors continue to adapt their operating models and tactics to maximise the profit they can extort from high-profile victims.

Countries with wealthier economies in North America and Europe are attractive targets and routinely top industry lists of states where incidents are most prevalent – although India, the United Arab Emirates, and Saudi Arabia also regularly feature. Access to cryptocurrency exchanges, dark web forums, and anonymous virtual private servers (VPS) provide the infrastructure behind the criminal ransomware industry. A growing cyber insurance market and larger ransom payments contribute to higher revenues for ransomware actors, who reinvest their earnings to develop new malware and research new targets.

A **Virtual Private Server (VPS)** is a portion of a large physical server divided into virtual spaces available for temporary use. Users worldwide can anonymously lease virtual private servers from a hosting company instead of operating their own physical hardware. The rental or subscription period for VPS services can be very short, meaning malicious cyber actors can move quickly from one set of infrastructure to another at a very low cost. Malicious users can move across jurisdictional boundaries and operate from anywhere using a VPS.

Major publicly reported ransom incidents in early 2021

MARCH 2021

India: Maharashtra Industrial Development Company

Spain: State Public Employment Service

Australia: Public Health Services in Melbourne

APRIL 2021

Slovakia: Slovakian Public Administration Organisations

Netherlands: Bakker Logistiek

Taiwan: Quanta Computer

Brazil: Rio Grande do Sul Court System

MAY 2021

US: Colonial Pipeline

Germany: Brenntag

Ireland: Health Service Executive

US: JBS Foods

Aotearoa New Zealand: Waikato DHB

France: AXA Asia Division

JUNE 2021

Belgium: City of Liege

Canada: Humber River Hospital

Japan: Fujifilm

US: University of Florida Health

In May 2021, the Colonial Pipeline Company proactively halted gas supply to the East Coast of the United States (US) after a ransomware incident impacted its billing system. The company confirmed they paid the DarkSide group a ransom of NZ$6.4 million worth of Bitcoin. German chemical distribution company Brenntag also reportedly paid the DarkSide group a similar amount in May 2021 after the group stole and threatened to leak private information. A month later, in June 2021, the US subsidiary of JBS Foods – the world's largest meat supplier – paid a ransom of NZ$16 million following a REvil compromise.

In addition to targeting commercial businesses with a low tolerance for service disruption, actors also target institutions with valuable research assets or large stores of personally identifiable information, such as universities.

Public sector organisations are not immune to ransomware; incidents against healthcare organisations were prevalent in 2021. While Aotearoa New Zealand responded to the May 2021 ransomware incident against the Waikato DHB, the Health Service Executive in Ireland reported severe disruptions to its health and social care services after a REvil compromise. In Australia, Canada, and the US, health services providers also suffered service disruptions in the wake of ransomware incidents.

The NCSC advises organisations never to pay a ransom or engage with extortionists. Paying a ransom funds the global ransomware industry, and there is no guarantee the actor will restore services or return stolen data.

Governments worldwide increasingly consider the prevalence of ransomware to be a national security issue because of the high risk of social and economic harm. In response, a combination of efforts to counter the problem are emerging.

Extortion tactics

An emerging tactic of ransomware actors is the use of multiple approaches to extort higher payments from victims. This so-called 'double extortion' and 'triple extortion' activity aims to increase pressure on victims and induce panic among decision makers. In addition to locking or encrypting files to disrupt a system, and then demanding a ransom in exchange for service restoration, actors now commonly access and exfiltrate sensitive data from networks prior to deploying malware. Actors will threaten to leak or sell the data if the ransom demand is not met. Actors may also directly contact media outlets or lists of customers to inform them about the data theft, and will use any public attention to pressure their victims. Some actors have attempted to extort money from downstream individuals or companies whose information has been stolen from the primary victim of the malicious cyber activity.

Cryptocurrencies enable criminal actors to extract and launder their profits, and to finance their ongoing and increasingly well-resourced operations. The increasing use of cryptocurrencies also enables cyber criminals to launder their proceeds of crime, often without detection.

Holding states publicly accountable for conducting, supporting, tolerating, or failing to adequately police ransomware actors will likely become more common in future. In July 2020, the European Union exercised its cyber sanctions regime for the first time, imposing targeted restrictive measures against individuals and companies involved in 'WannaCry' (a 2017 ransomware incident that severely impacted the UK's National Health Service) and 'NotPetya' (another 2017 incident). In 2018, the US Department of Justice issued federal indictments against individuals from the Democratic People's Republic of North Korea (DPRK) for their involvement in WannaCry. In February 2021, a United Nations (UN) panel of experts reported the DPRK continues to use cyber crime operations to evade sanctions and generate revenue in support of its nuclear weapons programme.

On behalf of the New Zealand Government, the Director-General of GCSB has joined international partners in condemning reckless, indiscriminate, and disruptive ransomware campaigns. In December 2017, the GCSB expressed concern about the involvement of DPRK cyber actors in the WannaCry campaign. In February 2018, the GCSB issued a statement adding Aotearoa New Zealand's voice to international condemnation of the NotPetya ransomware incident, which was attributed to Russia.

Supplier vulnerabilities

Supply Chain Cyber Security is the practice of identifying, assessing and managing cyber security risks in the supply chain.

A **Supply Chain Compromise** targets software, hardware, or an IT service provider with the ultimate aim to exploit downstream customers.

The increasing prevalence of cloud-hosted environments and supplier-managed services makes efficient, high-quality technologies accessible to more organisations. However, it can also reduce the control and visibility organisations exercise over their networks and the people who access them. The global, borderless market for technology has the potential to create dependencies and single points of failure. Geographically distributed software development and hardware manufacturing processes add to the complexity of the IT supply chain.

In the 2020/21 year, two high-profile global incidents emphasised the criticality of supply chain cyber security. In April 2021, Aotearoa New Zealand issued a statement supporting the international condemnation for the SolarWinds Orion incident, and agreeing with partner assessments that Russian state-sponsored actors were responsible for the supply chain compromise. Aotearoa New Zealand's condemnation of the activity echoed that of Australia, the UK, Canada, the US and the European Union: the widespread and indiscriminate deployment of malicious code undermined security and forced organisations to implement costly mitigations.

In early March 2021, Microsoft published a security advisory revealing a group they attributed to state-sponsored actors from the People's Republic of China (PRC) was exploiting a zero-day vulnerability in on-premises instances of Microsoft Exchange Server. Medium and large sized organisations commonly use Exchange Server to manage email and calendar services for their staff.

In the days following Microsoft's announcement, thousands of organisations around the world were similarly compromised by a variety of malicious cyber actors, including criminals, who quickly adopted methods of exploiting the vulnerability. The incident's widespread and indiscriminate impact illustrated the recklessness of targeting popular critical suppliers of products that many organisations rely on to conduct their business. The NCSC assisted a number of organisations affected by the activity, and in July 2021, Aotearoa New Zealand issued a statement alongside international partners criticising the PRC's use of the vulnerability, and indiscriminate sharing of the zero-day with multiple malicious cyber actors.

Rapid, sometimes automated, exploitation of CVEs continues to present challenges for network defenders. As organisations knit together popular software and hardware from global suppliers, they lose sight of managing which vulnerable and outdated products are running on their networks. State-sponsored and criminal groups have rushed to exploit this weakness. The impacts of widespread and reckless campaigns are widely felt, especially when they affect tools that have become fundamental to the IT supply chain.

The SolarWinds Orion supply chain compromise

In December 2020, a large number of public and private organisations were the victims of a sophisticated supply chain compromise. The compromise affected SolarWinds Orion – an IT systems management platform. Malicious cyber actors accessed and modified the code behind the company's software to insert their own functionalities. Platform users who later downloaded and installed SolarWinds Orion software updates unwittingly introduced the malicious code into their networks. The malicious code enabled backdoor access to a broad set of victims and allowed the actors to target a smaller subset for espionage. The compromise was later publicly attributed to Russian state-sponsored actors.

Disinformation

Disinformation is the deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose. Misinformation, in contrast, is incorrect or misleading information that is not produced and distributed with an underlying purpose. Circulating disinformation is a tactic sometimes used by state-sponsored actors to create confusion or erode social cohesion. While the NCSC is responsive to reporting from its security partners and the public regarding disinformation campaigns, the NCSC's role in responding is very limited.

Malicious cyber actors both rely on and enable the spread of disinformation. Over the 2020/21 year, the increase in COVID-19-themed disinformation and medical misinformation had a significant impact in the context of cyber security, where misinformation is used as a social engineering tactic. Public fear, interest, and desire for information about COVID-19 were exploited through pandemic-themed phishing lures and malware. In one instance, Avast – a security company and anti-virus provider – identified fake organisations using the World Health Organisation's logo and claiming to sell cures for COVID-19.

> The false information about a cure was spread as part of the actors' attempts to manipulate users into downloading malware.

Some states have increased their disinformation and political interference efforts and investment. The NCSC assesses the use of disinformation will likely continue to escalate. The rapid growth of artificial intelligence and the growing ease of access to virtual online services and infrastructure contribute to the issue. Technology companies play the most significant role in monitoring the integrity of data online. These companies are increasingly designing ways to detect and take down fake or machine-generated content. There have been a number of recent high-profile disinformation campaigns in cyberspace relating to democratic processes, including the 2016 US Presidential Election and the 2017 French Presidential Election. In the context of elections, disinformation presents considerable challenges because the spread of false information about election processes can compromise public trust and disrupt election administration. This has motivated some states – including Aotearoa New Zealand – to condemn such activity.

International norms

In December 2020, the New Zealand Government issued a position statement about how international law applies to state activity in cyberspace. In issuing the statement, Aotearoa New Zealand joined a range of countries that have articulated their positions on, and interpretation of, the international law, rules and norms governing state conduct in cyberspace. The NCSC gives operational effect to Aotearoa New Zealand's international commitments by identifying activity that is contrary to expected norms, and supporting the New Zealand Government to hold states to account when norms are violated. Clarifying states' rights and responsibilities in cyberspace forms a critical part of managing threats to Aotearoa New Zealand networks.

CONCLUSION
Whakakapi

Attempts to compromise Aotearoa New Zealand's networks are relentless, but continued technological innovation and digital interconnectivity bring huge benefits. Good cyber security practices will ensure Aotearoa New Zealand continues to prosper despite the growing sophistication and audacity of malicious cyber actors.

In the year ahead, the ability to prevent incidents and detect malicious cyber activity before harm happens should be a priority for any organisation that relies on or provides a digital service. Defences will need to be coordinated, acknowledging the interdependencies of all Aotearoa New Zealand organisations – from those who generate power, to those who move goods, host data, process financial transactions, provide education, or protect health and wellbeing.

While the 2020/21 year has seen a number of significant and harmful incidents, the NCSC has also observed a growing public awareness and understanding of the importance of cyber security. Good business leaders and decision makers across all sectors are alert to the challenge. Many are working collaboratively to make it difficult and costly for malicious cyber actors to profit from targeting Aotearoa New Zealand's networks.

The NCSC has a range of resources available to support organisations as they build and maintain secure, trusted, resilient networks:

- *Charting Your Course: Cyber Security Governance* defines the principles of a cyber security programme, including building a strong security culture, establishing roles and responsibilities, and embedding effective risk management.
- *Incident Management: Be Resilient, Be Prepared* works through five steps for establishing an incident management capacity. To make good decisions and recover quickly from incidents, organisations must plan and rehearse for the worst-case scenario.
- *Supply Chain Cyber Security: In Safe Hands* lays out the three phases of effective supply chain risk management; this will help organisations identify and protect key information assets and information flows, and manage the suppliers involved in protecting them.

While the NCSC continues to work to defend Aotearoa New Zealand's nationally significant organisations, we also seek to understand what threats will challenge us in the future, and how to plan for what may come. The consent and cooperation of our customers and partners makes it possible for the NCSC to have visibility over the cyber threat landscape. Through continued cooperation and effort, the NCSC will be able to meet the strategic objectives that serve and support the security and wellbeing of New Zealanders.

Getting in touch

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

The resources and guides mentioned in this report can be found on the NCSC's website.

If you would like to report a cyber security incident, or to access any of the general guidance referred to in this report, please visit our website: www.ncsc.govt.nz

GLOSSARY

Rarangi kupu

This glossary of terms is 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 / KUPU	DEFINITION / WHAKAMĀRAMATANGA
Advanced Persistent Threat (APT) | Tuma pakepake arā atu anō	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 publicly disclosed, as well as self-discovered, vulnerabilities.
Cloud Service | Ratonga kapua	Provides ubiquitous, convenient, on-demand access to shared pools of computing resources (such as servers, storage, or online applications).
Common Vulnerabilities and Exposures (CVE) | Whakaraeraetanga	A vulnerability is a weakness in software, hardware, or a network that can be exploited by an actor. The Common Vulnerabilities and Exposures (CVE) database is a publicly available register of known vulnerabilities, each assigned a unique identifier in the format of CVE-xxxx-yyyy.
Credentials | Whakatūturu pārongo	A user's authentication information used to verify identity – typically a password, token, or certificate.
Cyberspace | Āteatāurungi	The global network of interdependent information technology infrastructures, telecommunication networks, and computer processing systems in which online communication takes place.
Data Breach | Raraunga wāwāhi	The intentional or unintentional release of sensitive or private information into an unsecure environment.
Denial of Service (DoS) | Whakakore ratonga	An attempt to make an online service unavailable by overwhelming the service with more traffic than it can handle.
Exfiltration | Tāhae	Where an actor has unauthorised access to private organisational data (for example, legitimate credentials or intellectual property), and copies it from a system.
Incident | Maiki	An occurrence or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.

<table>
<tr><th>TERM / KUPU</th><th>DEFINITION / WHAKAMĀRAMATANGA</th></tr>
<tr><td>Malicious Cyber Actor | Nanakia tūkino mōhiohio</td><td>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.</td></tr>
<tr><td>Malware | Pūmanawa kino</td><td>Malicious software or code intended to have an adverse impact on organisations or individuals’ data, such as viruses, Trojans, or worms.</td></tr>
<tr><td>Mitigation | Ārai mōrea</td><td>Steps that organisations and individuals can take to minimise and address cyber security risks.</td></tr>
<tr><td>Nationally Significant Organisation | Whakahaere Hira ā-Motu</td><td>Organisations such as government agencies, key economic generators, niche exporters, research institutions, and operators of critical national infrastructure.</td></tr>
<tr><td>Personal Information | Ngā Mōhiohio Whaiaro</td><td>Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.</td></tr>
<tr><td>Phishing | Hītinihanga</td><td>The use of fake, deceptive, or alluring emails to solicit a behaviour from the recipient – such as clicking a link or divulging personal information or credentials.</td></tr>
<tr><td>Ransomware | Pūmanawa utu uruhi</td><td>A type of malicious software (malware) designed to disrupt the use of computer systems and files until a ransom is paid.</td></tr>
<tr><td>Supply Chain Compromise | Poke Ara Ratonga</td><td>A form of compromise that targets software, hardware, or an IT service provider, where the ultimate aim is to exploit downstream customers.</td></tr>
<tr><td>Virtual Private Server (VPS) | Tūmau Tūmataiti Mariko</td><td>A portion of a large physical server divided into virtual spaces available for temporary use.</td></tr>
</table>

GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI