Cyber Threat Report 2022/2023

National Cyber Security Centre

The National Cyber Security Centre is part of the Government Communications Security Bureau

Te Tira Tiaki
Government Communications
Security Bureau

CONTENTS

Ngā kaupapa

FOREWORD

Whakapuakitanga

The National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), supports nationally significant organisations to improve their cyber security posture and responds to national-level harm. This report provides our insight into the domestic and international cyber threat landscapes, and the incidents to which we responded over the past fiscal year.

In the 2022/2023 year, the NCSC recorded 316 cyber security incidents we disrupted, detected, or advised on. The proportion of financially motivated activity has exceeded state sponsored activity for the first time and the criminal activity we observe has greater potential impact to New Zealand's wellbeing.

Organisations in Aotearoa New Zealand are defending against an increasingly complex cyber threat environment. We see heightened determination from cyber-criminal actors attempting to extort payment from organisations that are increasingly aware of – and resilient to – extortion and manipulation tactics. Meanwhile malicious cyber actors are adopting new techniques and technologies, challenging orthodox detection methods.

With the rapid arrival of emerging technologies like generative artificial intelligence (AI), organisations seeking to benefit from these advancements must be prepared to govern their use, and control for privacy and security risks associated with their adoption.

The NCSC continues to adapt in order to better position the nation to respond to this rapidly changing environment. This reporting year we estimate NCSC advice and capabilities prevented $65.4 million in harm to nationally significant organisations. Over the last four fiscal years, the number of incidents detected by NCSC capabilities accounted for about a third of total recorded incidents.

In June, we supported the provision of our award-winning disruption capability, Malware Free Networks® (MFN®), to defend the customers of a major telecommunications provider. As the result of growing partnerships, our cyber threat intelligence now directly protects millions of New Zealanders and their businesses.

Recently, Cabinet directed the integration of NCSC and New Zealand's Computer Emergency Response Team (CERT NZ) functions to form the lead operational cyber security agency for Aotearoa New Zealand. By bringing together our people, capabilities, and domestic and international partnerships, New Zealanders stand to benefit from the consolidation of our mandates, along with a consistency of advice, and clearer knowledge about where to turn in the event of a cyber security incident.

> “Domestically, and internationally, we see heightened determination from cyber criminal actors attempting to extort payment from organisations.”

This report offers actionable insights into Aotearoa New Zealand's cyber threat environment, including mitigations to recurring tactics malicious cyber actors used effectively in high-impact incidents over the reporting year. We encourage organisations to use these to identify opportunities to uplift their cyber resilience when they review their cyber security controls and governance – and to reach out for further support as needed.

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

BY THE NUMBERS

Mā ngā tau

316

incidents affecting nationally significant organisations

(COMPARED TO 350 INCIDENTS RECORDED IN 2021/2022)

73

of those, or 23%, indicated links to suspected state-sponsored actors

(COMPARED TO 34% IN 2021/2022)

THE NCSC IN A TYPICAL MONTH*

Detects 7 cyber incidents affecting one or more nationally significant organisations through the NCSC's cyber defence capabilities.

Receives 20 new incident reports or requests for assistance. Of the new incident reports received each month, 12 come from international and domestic partners while 8 come from victim organisations self-reporting.

$382m

Since June 2016, the NCSC has prevented an estimated $382.4 million worth of harm to Aotearoa New Zealand's nationally significant organisations. $65.4 million worth of harm prevented in 2022/2023.

THE NCSC INCREASED AOTEAROA NEW ZEALAND'S COLLECTIVE CYBER RESILIENCE

Delivered **79** incident reports to customers

Published **7** advisories for customers, including 5 co-authored with domestic or international partners

Triaged **105** common vulnerabilities and exposures (CVEs), leading to 20 critical vulnerability alerts

Co-chaired **22** sector-based Security Information Exchanges

90

incidents, or 28%, were likely criminal or financially motivated

(COMPARED TO 23% IN 2021/2022)

250,000

In 2022/2023, the NCSC disrupted over 250,000 malicious cyber events as part of Malware Free Networks.®

IN THE 2022/2023 YEAR THE NCSC AND GCSB

Received 159 notifications of network change proposals under the Telecommunications (Interception Capability and Security) Act 2013 (TICSA).

Conducted 20 assessments of regulated space activities under the Outer Space and High-altitude Activities Act 2017 (OSHAA). Conducted 45 assessments of regulated radio spectrum activities under the Radiocommunications Act 1989.

Conducted 42 assessments under the Overseas Investment Amendment Act 2021 (OIAA).

* These numbers represent the incidents that meet the threshold for an NCSC response. Our focus is on incidents with a possible high national impact, or incidents that may affect Aotearoa New Zealand's nationally significant organisations. For incident reports that do not meet the threshold for an NCSC response, the NCSC engages with other domestic partners better placed to support the victim organisation.

OVERVIEW

Tirohanga whānui

The 2022/2023 Cyber Threat Report provides the NCSC's perspective on domestic and international cyber threat landscapes for the year beginning 1 July 2022 and ending 30 June 2023 (the fiscal year). The NCSC's understanding of the Aotearoa New Zealand cyber threat landscape is shaped by its focus on significant cyber threats leading to possible national-level harms, together with its unique capabilities and partnerships.

The growing availability of effective malicious cyber tools, compromised credentials, and vulnerabilities in public-facing infrastructure has made it easier for malicious cyber actors to work at scale, and with the sophistication required to cause national-level harm. It is likely more politically or ideologically motivated groups and individuals have access to the cyber tools they require to cause real-world impacts, and they are further galvanised by domestic and global events. The effects of Russia's invasion of Ukraine in February 2022 continue to be felt in cyberspace, too. While the direct cyber threat to Aotearoa New Zealand has not changed as a result of the invasion, the number and frequency of destructive or disruptive malicious cyber incidents globally has likely increased.

The first section of this report provides the NCSC's view of cyber threats affecting Aotearoa New Zealand. Based on our observations of the domestic cyber threat landscape, the report also provides advice on the steps organisations can take to mitigate the most significant threats seen this year. We work every day to protect Aotearoa New Zealand's prosperity and security through the provision of trusted cyber security services. However, all organisations play a part in protecting New Zealanders' privacy and security by adopting good cyber security practices.

Some of the key themes we explore include the continued effects of cyber criminal activity and extortion. We see ransomware imposing significant costs and requiring substantial recovery efforts. We increasingly see malicious cyber activity with downstream impacts, as Aotearoa New Zealand's digital supply chain is only growing in depth and interconnectedness. Phishing and other forms of social engineering are ubiquitous and effective. However, new techniques and emerging technology such as generative AI will almost certainly enable more convincing and targeted lures, potentially leading to a heightened pace of compromise.

During the 2022/2023 year, the NCSC contributed to several cyber security advisories, publicly identifying sophisticated malicious cyber activity and providing steps to detect and mitigate its impact.

In May 2023, we joined international cyber security partners in disclosing technical information about malicious software (malware) associated with Russia's Federal Security Service (FSB). In the same month, the NCSC joined its like-minded partners to identify techniques associated with the stealthy compromise of critical infrastructure. By 'living off the land', sophisticated cyber actors from the People's Republic of China (PRC) were able to use legitimate tools existing on victim networks to maintain access to significant targets overseas, without detection.

> "We increasingly see malicious cyber activity with downstream impacts, as Aotearoa New Zealand's digital supply chain is only growing in depth and interconnectedness."

The NCSC also continued to expand the coverage of its MFN® threat detection and disruption service, by adding new partners. A major milestone was the delivery of MFN to a telecommunications service provider's domestic customer base, reaching a significant proportion of the Aotearoa New Zealand mobile telecommunications market. These increasing and deepening partnerships mean the NCSC is offering unprecedented threat protection, with millions of New Zealanders now benefitting from MFN. Through anonymised reporting derived from MFN partners, the NCSC is developing its understanding of the cyber threat environment as it affects a significant segment of New Zealanders. We look forward to providing additional insights in time.

This report also identifies trends in the international cyber threat landscape, over which Russia's invasion of Ukraine still casts a shadow. A theme of the reporting year has been the rise of issue-motivated malicious cyber actors on both sides of the conflict. The NCSC remains concerned about unintended impacts as a result of disruptive malicious cyber activity stemming from the Russia-Ukraine conflict. Elsewhere, the discovery of a range of new botnets, as well as high-impact extortionate activity, threats to the security supply chain, and the convergence of information operations with malicious cyber activity have caused concern. Meanwhile, international law enforcement coalitions have also successfully imposed costs on cyber criminal operations.

The NCSC continues to observe a complex cyber threat environment. The sophistication and persistence of malicious cyber actors, both state-sponsored and financially motivated, continue to lead to significant cyber events. Additionally, the blurring distinction between state-sponsored and criminal cyber activity continues to increase, creating challenges for cyber investigators to understand the motives of malicious cyber actors.

Botnets

Botnets are normally networks of compromised personal or office devices such as internet modems, personal computers, or network attached storage. Malicious cyber actors use these as infrastructure to send spam, perform denial-of-service activities, or attempt to obfuscate the origins of a malicious cyber campaign.

For more information about NCSC services or guidance, visit our website (www.ncsc.govt.nz).

For readers unfamiliar with any of the terms used, or how the NCSC defines them, a glossary is provided on page 23.

Cyber Security Emergency Response Plan (CSERP)

The CSERP sets the framework for the Government's response to a cyber security emergency.

For more information see: dpmc.govt.nz/publications/new-zealands-cyber-security-emergency-response-plan

ABOUT OUR WORK

Mō ā mātou mahi

Our people work at the heart of Aotearoa New Zealand's cyber defence. Our mission is to protect Aotearoa New Zealand's wellbeing and prosperity through trusted cyber security services.

Our strategic objectives

- Defend National Security
- Raise Cyber Resilience
- Facilitate Digital Transformation

Every day, we work to protect Aotearoa New Zealand and its interests. The NCSC supports nationally significant organisations to improve their cyber security, and we respond to national-level harm and advanced threats.

We provide system leadership for government cyber security. One of the ways we provide leadership is by developing standards and frameworks for Aotearoa New Zealand organisations, including the NCSC Cyber Security Framework (the framework). The framework is a way of organising cyber security activities, and provides a common language to describe them. In developing our guidance, we engage with international standards bodies and keep up-to-date with new approaches and challenges, which we take into account as we author the New Zealand Information Security Manual (NZISM).

Our detection and discovery focus is on cyber threats with the potential for national-level harm, or affecting nationally significant organisations.

This includes working with significant public and private sector organisations to deploy defensive capabilities, including our suite of CORTEX capabilities.

When cyber security incidents happen, we take action to reduce the impact and minimise future harm. We provide insights about the cyber threat landscape through public advisories and classified assessments. We uplift cyber resilience throughout Aotearoa New Zealand, which, in turn, increases the costs to adversaries targeting

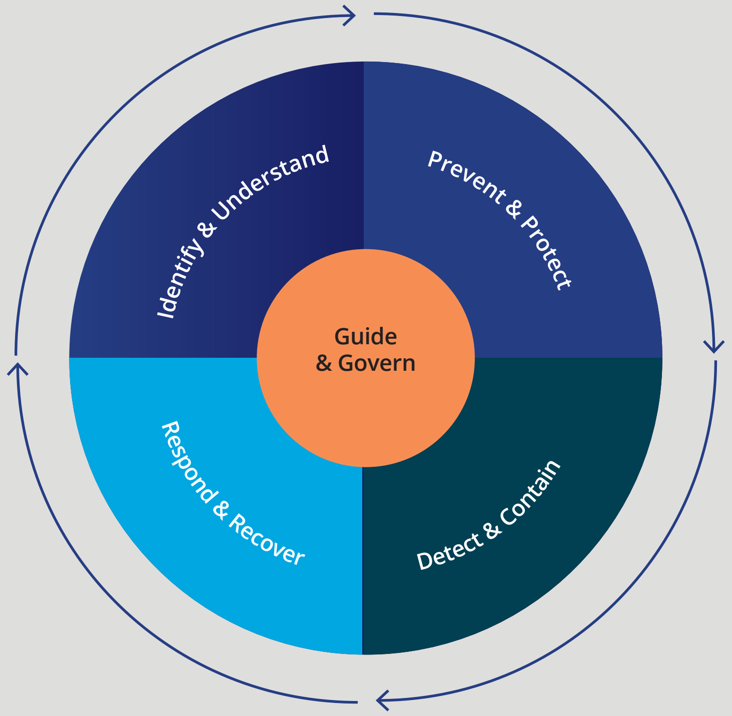
The NCSC Cyber Security Framework

The framework includes five functions:

- Guide & Govern
- Identify & Understand
- Prevent & Protect
- Detect & Contain
- Respond & Recover

Organisations can refer to the framework to understand how the NCSC uses advice, guidance, standards and security services to communicate consistently what being cyber secure and cyber resilient means. In this report, we will refer to the NCSC Cyber Security Framework and its functions.

For more information see: ncsc.govt.nz/resources, where the framework is available to use under a creative commons licence.



domestic systems. During the 2022/2023 year, the NCSC delivered a total of 79 incident reports to specific customers, and provided seven general advisories or guides.

The NCSC is in a period of transformation. As Ministers announced in July 2023, we are in the early stages of moving to a new operating model, with the establishment of a lead government operational cyber security agency. This involves the integration of the functions of the NCSC and CERT NZ, from 31 August 2023. Our people continue to deliver their existing core functions to their current customers, while supporting this change. We look forward to increased collaboration over time as we move toward a single integrated operational agency.

Who we work with

The NCSC is at the heart of national cyber defence, but people and partnerships are key to preventing harm from malicious cyber activity in Aotearoa New Zealand. We work with domestic and international agencies to understand the cyber threat landscape, respond to incidents, and give robust cyber security advice. We also work with commercial partners to deliver key services.

In 2022/2023, some of our key domestic partners included CERT NZ, which supports individuals and businesses to understand cyber threats and respond to incidents, the Department of Internal Affairs (DIA), responsible for digital safety and reducing spam, and New Zealand Police, which investigates digital crime. We further provide all-source strategic cyber intelligence and advice government-wide, including to the Department of Prime Minister and Cabinet's (DPMC) National Cyber Policy Office (NCPO), the Ministry of Foreign Affairs and Trade (MFAT), the Ministry of Business Innovation and Employment (MBIE), New Zealand Defence Force (NZDF), DPMC's National Assessments Bureau (NAB), and the New Zealand Security Intelligence Service (NZSIS).

We maintain strong international relationships to share intelligence and understand the cyber threat landscape. We work closely with the Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), the United Kingdom's National Cyber Security Centre (UK NCSC), the United States (US) National Security Agency Cybersecurity (NSA Cybersecurity) and the US Cybersecurity and Infrastructure Security Agency (CISA).

We work with information technology organisations and cyber security providers to investigate cyber compromises, provide advice about how commercial services meet the needs of their government customers, and to deliver MFN®.

MFN partners are key to the service's success. Partners deploy the threat detection and disruption capabilities to the core and the periphery of hundreds of customer networks – ensuring that when threats are identified, they are quickly disrupted. As at 30 June 2023, the NCSC has 14 commercial partners delivering MFN services: Advantage, Cassini, CyberCX, Datacom, Defend, Inde, InPhySec, The Instillery, Scientific Software & Systems, Kordia, Liquid IT, One NZ, Spark, and Unify. We are also working with additional industry partners to identify opportunities to expand MFN's protective reach.

Acknowledgement for MFN®

The GCSB's Malware Free Networks® (MFN®) capability has received industry praise. MFN won the "Best Security Product or Service" at the annual iSANZ cyber security industry awards in November 2022. The judges noted MFN helps defend against an evolving range of cyber threats and has increased the cyber security resilience of many New Zealand organisations. Additionally, the judges commented on the strength of MFN's design and implementation, and its ability to improve security across the country while also protecting the privacy of users.

MFN was also the recipient of the 2023 Te Tohu a te Pirimia, Prime Minister's Award at the Te Hāpai Hapori, Spirit of Service awards. In addition, the threat detection and disruption service was also joint winner of the Te Tohu mō te Ratonga Whakahirahira, Service Excellence award. The awards recognise the collaborative approach MFN uses to raise Aotearoa New Zealand's cyber defence.

AOTEAROA NEW ZEALAND THREAT LANDSCAPE

Te āhuatanga o ngā tuma i Aotearoa

This section of the report identifies key cyber threat trends affecting Aotearoa New Zealand organisations in the 2022/2023 year. This includes more severe and significant financially motivated breaches, espionage, service provider compromises leading to the compromise of information related to multiple organisations, as well as the exploitation of remote working solutions and cloud services for malicious cyber activity.

2022/2023 NCSC incidents

This fiscal year we recorded 316 cyber security incidents. This figure is about 10% lower than the previous year. The difference may reflect a number of contributing factors, including: recent disruptions to cyber criminal infrastructure (see page 19 for more); changing priorities or tactics of states; organisational cyber resilience and maturity; and/or our increasing ability to disrupt activity before harm takes place. Developments in the NCSC's cyber defensive capabilities have allowed us to scale some services to a significant number of organisations, and even to protect individual home users.

The NCSC receives information about cyber security compromises or suspicious cyber activity from a number of sources, including its own detection and discovery capabilities, international cyber security partners, domestic agencies, and customers themselves.

Despite a drop in the total number of incidents recorded, including incidents reported to the NCSC by other organisations, the number of incidents detected by NCSC capabilities grew year-over-year. Viewed over the last four fiscal years, the number of incidents detected by NCSC capabilities accounts for about a third of our total recorded incidents.

A typical month this year saw the NCSC's MFN® service disrupting 20,800 connections to known malicious infrastructure; the NCSC detecting seven cyber incidents; and receiving 20 reports or requests for assistance. Of the incidents reported, the NCSC receives an average of 12 from domestic or international partners and eight self-reports from victim organisations themselves.

What's the harm?

In 2022/2023, the detection, disruption, advisory and threat intelligence services the NCSC provides prevented an estimated $65.4 million of harm to Aotearoa New Zealand's nationally significant organisations. This figure reflects incidents where the NCSC's detection of malicious cyber activity or engagement with victims likely prevented future harm.

The estimate is 98% higher this year than last. This reflects the advice we gave to organisations responsible for critical services – such as power, waste, and water where cyber incidents can be more impactful – or the NCSC's support to information technology (IT) managed service suppliers with various Aotearoa New Zealand government customers. In these cases, the compromise of one organisation could have significant downstream harms to several nationally significant organisations. Finally, in 2022/2023 the

How the NCSC defines incidents

An NCSC incident can be any threat to a nationally significant organisation's network or information – or where the activity has the potential to cause high national harm. This may occur even when 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 can all be counted among the NCSC's total incidents.

We categorise 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 (see page 8 for more).

NCSC was more readily able to verify that organisations took actions in response to our advice, which is a key factor in measuring our impact.

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 security incidents to specific sectors.

The model 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.

The pre-emptive and preventive nature of our MFN® capability means any malicious activity generally occurs at a point before its value is able to be reflected in this calculation. However, there were several instances in the 2022/2023 year where activity detected by the MFN capability was responded to as an incident. Typically, in such cases a compromise has already occurred and MFN is able to disrupt secondary effects of the compromise. Those incidents are reflected in this calculation.

Incidents by category

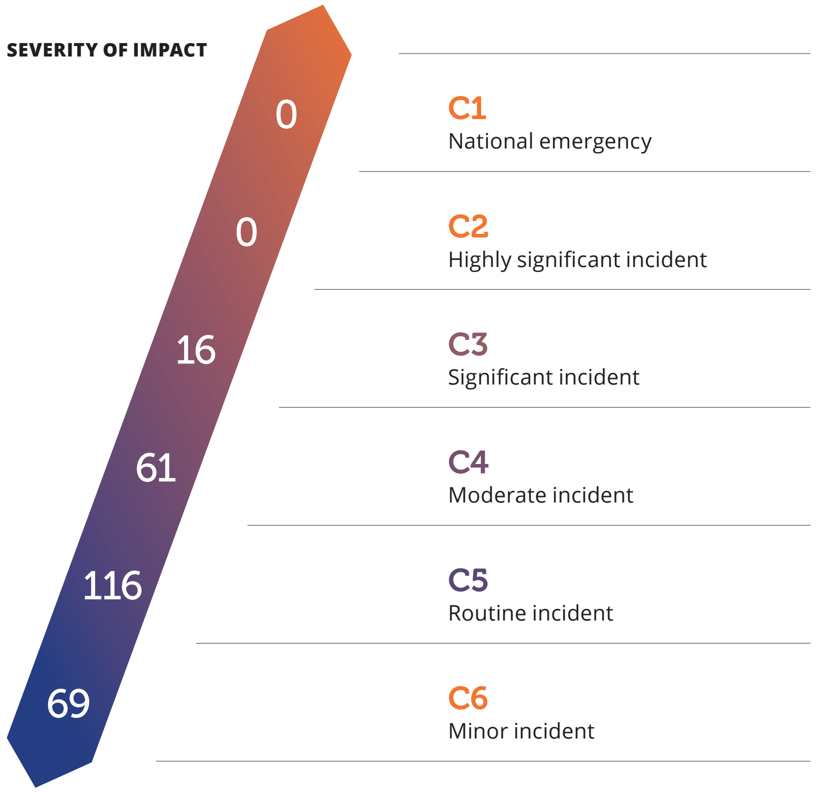
The total number of incidents is only part of the story. A handful of significant incidents in a fiscal year would more radically change the domestic landscape than hundreds of minor incidents because the potential impact on critical services, society, and the economy would be greater.

To help understand the impact of any one cyber incident, the NCSC triages incidents into categories, which consider the size of the organisation impacted and the severity of the compromise. A national cyber emergency (C1) is a cyber incident causing severe disruption to a core Aotearoa New Zealand service, and/or affects key sensitive data, and/or undermines the economic or democratic stability of Aotearoa New Zealand. To date, the NCSC has never responded to a C1 cyber incident. If one were to occur, it would demand a resource-intensive, multi-agency response, with the NCSC providing advice, coordination, and its technical capabilities.

On the other end of the scale, a minor incident (C6) is a cyber incident causing a known or likely impact to an individual/individuals, or precursor activity against an individual/ individuals or a small or medium enterprise. During a C5 or C6 incident the NCSC may be involved in providing advice or guidance to the organisations as they triage the incident and harden their defences for the future, or we may pass the investigation to CERT NZ to provide appropriate advice.

In the middle, a significant incident (C3) is an incident causing a known or likely impact on a large commercial enterprise, wider government, or supply chain to core Aotearoa New Zealand services. Even a C3 can require significant effort on behalf of the NCSC, as well as the victim and their cyber security and IT suppliers. The initial response can last weeks. These incidents tend to have a long tail for the victim – and sometimes for their customers, too.

Incidents by category for the reporting year



This year's most severe incidents were categorised C3. Unlike the 2021/2022 year, in which we recorded two C2 incidents, the 2022/2023 C3 incidents were predominantly associated with disruptive ransomware or other extortion activity. A number of these incidents had second-order effects for Aotearoa New Zealand organisations. For instance, the compromise of one organisation posed risks to the privacy and security of a number of other Aotearoa New Zealand organisations.

Another C3 incident began with the compromise of an internet-facing device in a local government organisation. While the device was likely compromised opportunistically, owing to the availability of known vulnerabilities in a commonly used security product, the malicious cyber actor successfully moved laterally within the victim's network. The NCSC alerted the organisation to the compromise, likely by a sophisticated malicious cyber actor seeking data for espionage purposes. Before detection and containment, the actor compromised a server and several devices belonging to the victim. The NCSC assisted the victim organisation and its IT managed service provider to understand the scope of the intrusion, remove the intruder and prevent further attempts to compromise their network. Prompt response efforts and work to identify the full path of the intrusion contained the compromise and reduced its impact.

Confidentiality

To protect relationships of confidence and trust, the NCSC does not generally comment publicly about whether it is involved in providing investigation or incident response support to victims of malicious cyber activity. The NCSC treats incidents reported to us in strict confidence. This helps to encourage organisations to engage with us when they have been subject to a cyber security incident. It also helps to protect the integrity of any investigations in which the NCSC is involved. There are occasionally highly significant incidents where the NCSC and the organisation/s we are assisting may agree that disclosure of our involvement is appropriate.

Disrupting malicious cyber activity

Aotearoa New Zealand calls out malicious cyber activity when it is in the national interest to do so. By providing examples of malicious cyber activity in public, Aotearoa New Zealand can raise awareness of the threat, and signal to nation states what it views as irresponsible behaviour.

The GCSB, through the NCSC, conducts robust technical attribution of malicious cyber activity affecting our national security and wellbeing. We usually provide these as classified assessments to the Aotearoa New Zealand Government for use in an all-of-government process determining our national response.

On some occasions, malicious cyber activity affects Aotearoa New Zealand's interests indirectly, or has the potential to affect us in future. In these circumstances, the NCSC may join international partners to produce advisories that identify malware or specific tactics, techniques and procedures (TTPs). These advisories raise awareness of the cyber threat and provide information to mitigate malicious cyber activity.

Increasingly, nation states are undeterred by a process of 'calling out' malicious cyber activity – in other words, being associated with malicious cyber activity. However, nations opposing the malicious use of cyber capabilities can take steps to impose real costs: providing indicators of compromise or identifying malware and behaviours to enable faster detection and incident response, thereby reducing the effectiveness of malicious cyber tools and infrastructure. This can have a profound levelling effect, benefiting the defenders of critical networks and services.

During the 2022/2023 year, the NCSC contributed to several cyber security advisories, publicly identifying sophisticated malicious cyber activity and providing steps to detect and mitigate its impact.

- In May 2023, we joined international cyber security partners in disclosing technical information about malware associated with Russia's Federal Security Service (FSB) and frequently used against sensitive intelligence targets. Together with partners in Australia, Canada, the United Kingdom and the United States, the NCSC provided information about the latest revision of malware known as 'Snake'.
- In the same month, the NCSC joined its like-minded partners to identify techniques associated with the stealthy compromise of critical infrastructure. By 'living off the land' sophisticated cyber actors from the PRC were able to use legitimate tools existing on victim devices and networks to maintain access to significant overseas targets without detection.

Living off the land
A technique using legitimate and pre-existing software on a victim network, in contrast to the installation of malicious software, to maintain network accesses. Use of legitimate software and accounts is less likely to raise alerts for defenders.

- In June 2023, the NCSC and partners identified tactics associated with the deployment of LockBit – the most pervasive ransomware worldwide, and with significant impacts in Aotearoa New Zealand. LockBit has affected government, energy, emergency services, healthcare and logistics sectors internationally. The advisory *Understanding Ransomware Threat Actors: LockBit* identifies the legitimate re-purposed tools and the MITRE ATT&CK® TTPs associated with LockBit actors.

In each of these cases, the NCSC supported the distribution of threat information – including through its co-chairing of Security Information Exchanges.

Security Information Exchanges (SIEs)

The NCSC facilitates information-sharing among organisations facing similar threats and challenges, especially where sharing requires a high level of trust. This primarily takes place through SIEs focused on specific aspects of Aotearoa New Zealand's critical infrastructure. SIEs are invitational trust groups for cyber security professionals in the energy, finance, government, network-provider, tertiary, and transport and logistics sectors.

MFN® by the numbers

14
Partners disrupting based on MFN threat intelligence.

390,000+
Total disruptions as part of Malware Free Networks since December 2020.

3
Partners on-boarded in the 2022/2023 year.

20,000+
Disruptions in a typical month.

Another key way we disrupt malicious cyber activity affecting Aotearoa New Zealand is through the provision of the MFN® threat detection and disruption service. In the 2021/2022 year, the NCSC launched the service, working with commercial cyber security and infrastructure partners to provide high-confidence malicious indicators that should be disrupted wherever they are detected.

With 14 industry partners offering MFN to their customers, including three new partners this fiscal year, 2022/2023 demonstrated the scalability of our defensive capabilities, with over 250,000 disruptions, including hundreds of disruptions associated with state-sponsored activity. As of 30 June 2023, MFN had disrupted more than 390,000 threats in total. This figure reflects disruptions of malicious activity with the potential to cause harm to Aotearoa New Zealand organisations and individuals.

Through MFN, the NCSC also supplied cyber defenders with indicators for a number of unique threats to Aotearoa New Zealand, including the impersonation of Aotearoa New Zealand organisations and government services – this activity contributed to over 20,000 disruptions.

In 2022/2023, the NCSC worked with partners One NZ and DEFEND to prepare the MFN service for scaling to One NZ's domestic broadband and mobile customers. With an increased reach of around two million people, we have provisionally observed a growth in reported disruptions of over 3,000% since June 2023.

[2] 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. For more information about the NCSC's use of MITRE ATT&CK, see page 14.

Who harms Aotearoa New Zealand?

In 2022/2023, 23% of incidents showed indications of a connection to state-sponsored actors (compared to 34% in the previous year). The total of 73 incidents is a decline on the 118 recorded in 2021/2022. This 61% decline contrasts with this year's record-high proportion of links to financially motivated groups or malicious cyber actors exhibiting financially motivated behaviours. For the first time, the NCSC recorded a higher proportion of financially motivated activity than activity with links to state-sponsored cyber actors.

About half of all incidents showed neither clear links to state-sponsored activity nor criminal activity. Some examples of these unattributed incidents involved two instances of distributed denial-of-service (DDoS) against a government organisation, and suspicious activity on the network of a managed service provider.

State-sponsored cyber actors primarily pose an espionage threat to Aotearoa New Zealand. These actors continue to demonstrate intent and capability to target Aotearoa New Zealand. State-sponsored cyber actors are typically motivated to maintain covert persistence on computer networks of high intelligence value. To achieve this goal, malicious cyber actors continue to identify novel weaknesses in – or new techniques for – evading Aotearoa New Zealand cyber defences.

Activity of this calibre against Aotearoa New Zealand networks is challenging to identify and to attribute with high levels of confidence to specific cyber actors. Attribution to specific states may not be possible with the information obtained in every incident response phase.

State-sponsored cyber activity is less likely to disrupt services or cause obvious harm, and less likely to enter the public spotlight, but still has potentially significant impacts to Aotearoa New Zealand.

State-sponsored malicious cyber actors typically target Aotearoa New Zealand to understand our diplomatic and policy positions, or to undertake commercial espionage supporting their economic development; this can involve theft of intellectual property from Aotearoa New Zealand organisations. State-sponsored malicious cyber activity may initially present as if conducted by a financially motivated actor and, at times, may actually be financially motivated. State-sponsored cyber actors may also indirectly affect Aotearoa New Zealand: given increasing global interconnectedness, and heightening geostrategic competition, activity affecting our like-minded partners may have downstream impacts for Aotearoa New Zealand.

The NCSC remains concerned about malicious cyber activity with suspected state backing affecting international critical infrastructure. We work closely with our international partners to identify and provide early warning to Aotearoa New Zealand organisations of activity that could have disruptive impacts here.

> "For the first time, the NCSC recorded a higher proportion of financially motivated activity than activity with links to sate-sponsored cyber actors."

In 2022/2023, the NCSC observed more criminally linked malicious cyber activity than in past years. Ransomware and extortion activity continue to comprise a significant portion of the confirmed criminal activity the NCSC observes. The number of ransomware incidents recorded by the NCSC has remained relatively constant over the last three years, but the impact to Aotearoa New Zealand has almost certainly increased. On average, the NCSC recorded more than one ransomware incident per month in the fiscal year, and half of these incidents were categorised as C3 (indicating a significant incident). One C3 incident posed a threat to operational technology. In this case, the networks for managing sensitive critical infrastructure were segregated, but the victim was still required to activate business continuity plans to ensure the continued safe running of their service. Such an incident highlights the pervasive threat to critical infrastructure if malicious cyber actors are able to move laterally from corporate networks into operational technology networks.

Over the 2022/2023 year, the NCSC observed malicious cyber actors increasingly taking advantage of exfiltrated data to extort payment from their victims. The theft of data, combined with encryption of the victim's copy, has been referred to as 'double extortion', as the malicious cyber actor now has two opportunities to leverage payment from the victim. This double extortion exponentially increases the potential harm an organisation experiences during these breaches. In 2022/2023, a number of larger organisations hosting critical services for customers downstream were impacted by ransomware. In one case, the NCSC responded to the ransomware of an IT managed service provider with a significant government customer base.

The NCSC also recorded a number of instances in which precursors to ransomware were detected and mitigated prior to the encryption or extortion phase. Increasing our ransomware detection posture – and detecting activity before significant disruption occurs – remains an NCSC operational priority for the coming years.

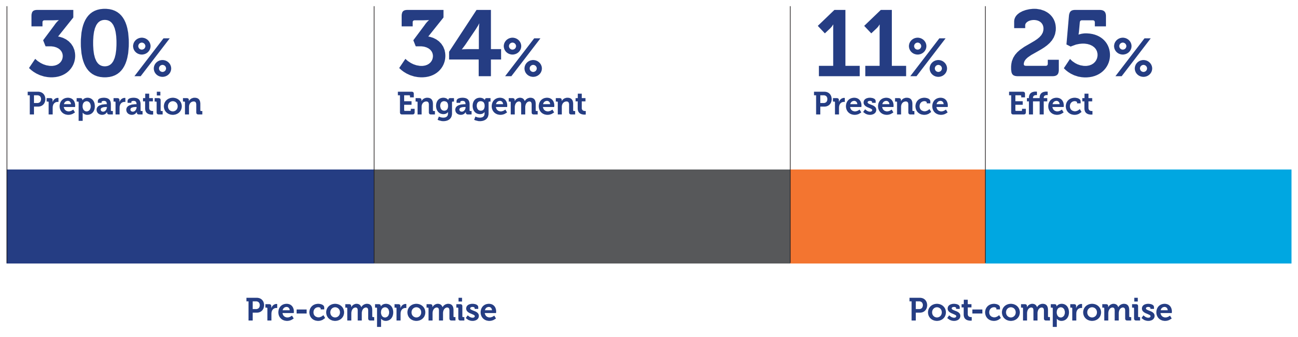
The NCSC recommends never paying cyber ransoms

Governments worldwide are increasingly concerned about appropriate protection of sensitive data, including personal information, and are discouraging or outlawing the payment of a ransom.

The Aotearoa New Zealand Privacy Act 2020 requires reporting of privacy breaches that have caused serious harm or are likely to do so. In 2021, Cabinet agreed government agencies should not pay cyber ransoms. Payment of a ransom could also be in violation of the Russia Sanctions Act 2022 or the United Nations Act 1946.

For more information see: ncsc.govt.nz/news/ransomware-advice

Representation of incidents by phase



Across all 2022/2023 incidents recorded by the NCSC, 64% of confirmed malicious activity likely did not pass the engagement phase to achieve a network compromise. This demonstrates the NCSC and its customers' capability to disrupt the majority of malicious activity, prior to it having an impact. This contrasts to 25% of incidents having a measurable effect on the organisation concerned. Effects in this case are most commonly data encryption for extortion, exfiltration of sensitive or operational data, disabling services, or hijacking computing resources for further malicious or illegal activity.

Pre-compromise activity is characterised by planning, reconnaissance or initial engagement with a victim – for instance via delivery of a phishing message. While pre-compromise incidents usually have a lesser impact on the organisations involved, they have potential to escalate if not detected and mitigated in a timely manner. Strengthening the first layer of cyber defence can have a significant impact in preventing a pre-compromise incident from escalating. In contrast, post-compromise incidents are discovered when the malicious cyber actor has established unauthorised access to a system, account or computer network. These incidents usually require significant remediation efforts. It is important to identify the access vector, persistence mechanism, and any lateral movements the cyber actor may have made, in order to be confident the remediation and eviction efforts have been effective. It is equally important to identify the data a malicious cyber actor may have had access to, or stolen, to understand the ongoing privacy risk. The most severe incidents are those where the adversary has achieved their desired goal, either by accessing sensitive information, hijacking resources for future malicious cyber campaigns, or by disabling or deleting data or services.

> "We have in the past year witnessed geostrategic competition intensifying right around the world, including in our Pacific region, while serious cyber incidents continue to threaten New Zealand organisations."

Andrew Hampton, Director-General, Government Communications Security Bureau, 27 March 2023 report to the Intelligence and Security Committee

Case study

In March 2023, the NCSC became aware of a supply chain compromise associated with software used by Aotearoa New Zealand organisations. By downloading a software update for a compromised desktop client, downstream victims would inadvertently install additional malware to act as a cryptocurrency miner. The NCSC provided advice to its customer base to mitigate the supply chain threat and ensured that relevant indicators of compromise were distributed via its disruption capability. One Aotearoa New Zealand nationally significant organisation likely downloaded a compromised version of the software, but secondary effects – such as the installation of the cryptocurrency miner – were highly likely blocked by the NCSC's MFN® service. The NCSC identified the compromise and engaged with the MFN partner to provide remediation advice.

Supply chain vulnerabilities

A supply chain compromise usually targets software, hardware, or an IT service provider, and the ultimate aim is to exploit downstream customers. Supply chain compromises can also occur when one organisation holds data for another.

Cyber criminals seeking to maximise profits may target victims they perceive to hold data on behalf of multiple organisations. Criminals may leverage the initial victim's reputation with their customers, threatening to expose the fact of a cyber security compromise; alternatively, criminals may seek an extortion payment from each owner of the stolen information. This year, the NCSC recorded an incident during which customers of a domestic service provider were approached for extortion separately from the initial victim.

Similarly, state-sponsored cyber actors are likely pre-positioning on networks globally to enable downstream campaigns. As it takes significant time and resource to maintain long-term, persistent access, many state cyber actors likely view a vulnerable link in a key supply chain as an efficiency.

Drawing on its unique capabilities, the NCSC works with critical infrastructure, providing alerts and advice to mitigate these potential threats.

Also in the 2022/2023 year, the NCSC supported several organisations whose providers' cyber security was compromised, exposing sensitive data. In such cases we can provide customers with strategic communications support, help them to understand the impact, and improve their digital supply chain management practices.

For more information, see ncsc.govt.nz/resources/cyber-resilience-guidance

Support to major events

The GCSB contributes cyber security support to multi-agency efforts on major national events. Planning for major events involves preparing for the possibility a cyber security incident could cause disruption or threaten the integrity of the lead organisation's sensitive data. In 2022/2023, through the NCSC, the GCSB provided cyber security support to a number of events, including the local body elections in October 2022, and the five-yearly Census led by StatsNZ in early 2023. We also began preparations to support the 2023 General Election, led by the Electoral Commission.

In each case, the NCSC established a bespoke plan of work to support the organisations involved, as well as key suppliers, and participants.

During the 2022 local government elections, the NCSC renewed its engagement with a range of involved organisations, provided advice to them, and contributed to incident response preparation. The NCSC provided proactive advice to specific local government organisations to mitigate their threat surface and reinforce their cyber defences. The NCSC provided advice to StatsNZ ahead of collecting for the 2023 Census.

The NCSC reviewed key cyber security documentation, participated in exercises to help inform their response plan, and provided tailored advice to reinforce their cyber defences. The NCSC also conducted proactive analysis using its unique cyber defence capabilities to identify any threats to the 2023 Census. StatsNZ also benefited from the NCSC's MFN threat detection and disruption service.

The NCSC supported Aotearoa New Zealand's General Election in 2023 and continues to look for opportunities to contribute cyber security expertise to other major national events.

Analysing trends in tactics and techniques

The NCSC uses the MITRE ATT&CK® framework to map cyber security incidents. By mapping recorded incidents to MITRE ATT&CK, the NCSC can gain insights into common or emerging trends in actor tactics and techniques. Each malicious incident can include multiple tactics and techniques, depending on the evidence of malicious activity.

Compared to last year, the NCSC observed a wider variety of TTPs in the cyber incidents it recorded. This may indicate that malicious cyber actors have become more resourceful, or that Aotearoa New Zealand's defensive posture has forced malicious cyber actors to adopt a more diverse range of TTPs to be successful.

Common preliminary techniques, such as vulnerability scanning or other reconnaissance, are often easy to detect and record. They frequently feature among the top 10 TTPs in NCSC records, although they do not always provide a useful barometer of the cyber threat. Sometimes, reconnaissance activity is merely passive information gathering. As in past years, vulnerability scanning remains in the top-recorded techniques.

> "Compared to last year, the NCSC observed a wider variety of TTPs in the cyber incidents it recorded."

Common Vulnerabilities and Exposures (CVEs)

Common Vulnerabilities and Exposures (CVEs) are publicly disclosed information security issues, stored in a database. A CVE number uniquely identifies each vulnerability. A 'zero-day' is a software vulnerability for which there is currently no patch, and for which there is often no CVE number assigned.

The NCSC triages vulnerabilities according to a number of factors. Vulnerabilities in software we know to be widely used in Aotearoa New Zealand's nationally significant organisations are given higher priority in our triage system. The NCSC uses this assessment to provide applicable advice and alerts to its customers. Timely and targeted advice enables patching before compromise. On at least one occasion this year, the NCSC has been the catalyst for a significant Aotearoa New Zealand organisation to address a security vulnerability.

Reconnaissance techniques are often used to identify weaknesses in internet-facing devices. They also likely provide malicious cyber actors with intelligence about where devices are located, even in advance of the existence of a software vulnerability. This intelligence may significantly reduce the time between a malicious cyber actor being aware of a vulnerability and being able exploit it for network access. The NCSC continues to observe scanning and exploitation at speed and scale in response to recently disclosed vulnerabilities. Malicious cyber actors often exploit vulnerabilities in internet-facing devices without a clear purpose or strategic intent. By gaining an initial foothold on hundreds of networks, malicious cyber actors can then continue the compromise lifecycle selectively, dependant on the assessed value of the vulnerable network.

Meanwhile in 2022/2023, the NCSC also detected an increase in phishing techniques. Despite the increase in observed phishing activity, this activity is rarely involved in the highest-severity cases the NCSC handles. Such cases usually include the compromise of multiple devices in a corporate or government network, and/or the theft of commercial or sensitive data. Instead, the majority of incidents involving phishing techniques were detected or disrupted before a serious network compromise occurred.

We have heightened concern about infrastructure compromised for use in botnets, including by state-sponsored actors. Compromised infrastructure may be used to obfuscate the location of a malicious cyber actor, or to amplify the effects of a denial-of-service campaign. This activity aligns with international reporting during the year: cyber defenders detected the presence of a number of unique botnets, usually made up of small office/home office (SOHO) or internet of things (IoT) devices (see page 20 for details). During 2022/2023, the NCSC had some success alerting customers when it became aware of their device's participation in a botnet.

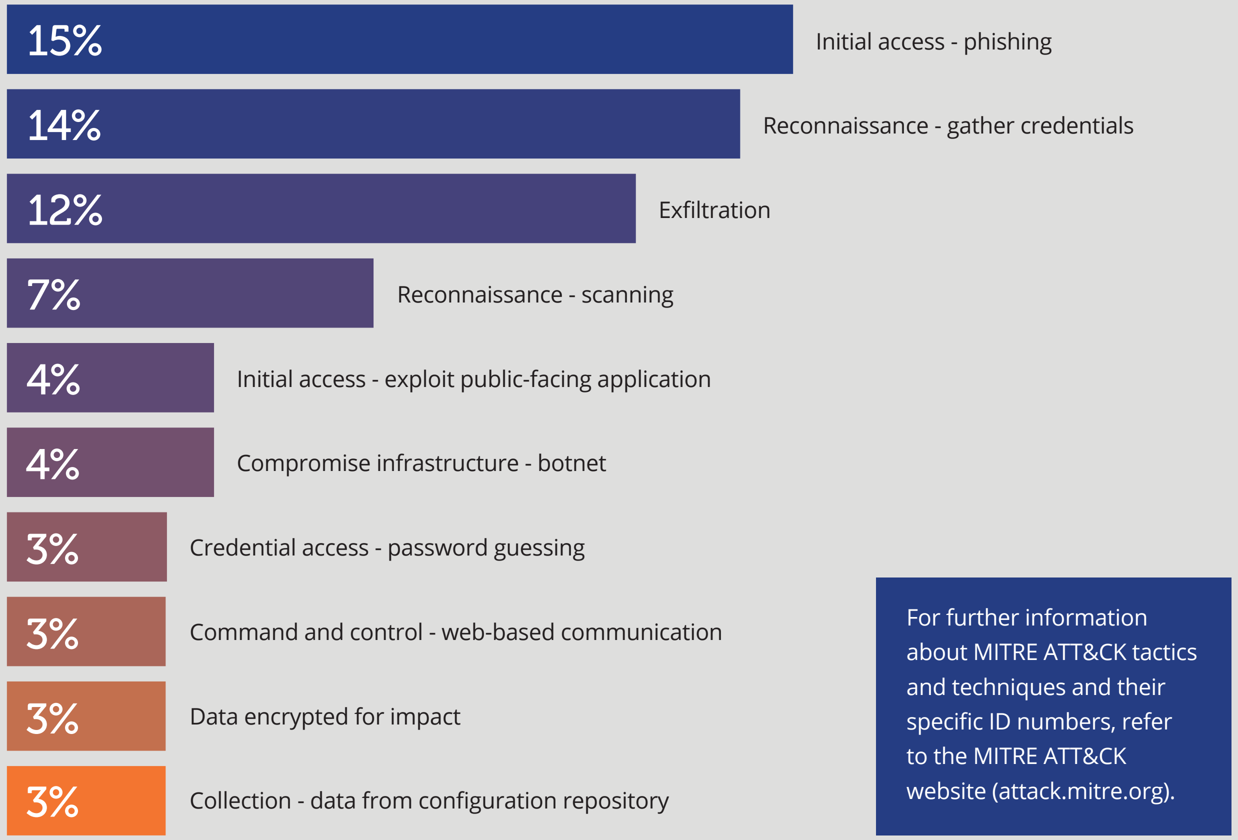
For years, a thriving market for stolen personal information and credentials (login and passwords) has existed as a mainstay of the 'dark web' – a subset of the internet that is not indexed by search engines and instead requires specialist knowledge or software to access. During 2022/2023, the NCSC saw an increase in the volume of compromised credentials, any one of which could contribute to a later network-wide compromise. It is rare to be able to link with confidence the theft of specific corporate credentials to a later, more serious compromise. However, the NCSC also observed a correlated increase in the use of legitimate credentials in routine and significant incidents in 2022/2023.

During the year, the NCSC undertook a review of Aotearoa New Zealand government identities appearing in data breaches since 2008, drawing on data from the 'Have I Been Pwned' service. Following this analysis, the NCSC provided 151 proactive alerts to organisations with official government top-level domains (govt.nz). The number of breached email addresses fluctuates, but peaked in 2019 with more than 57,000 instances of government emails found in data breaches. While not every breached data set contains both passwords and usernames, an email address is often enough to enable research in the reconnaissance phase of a malicious cyber campaign.

The NCSC also recorded a number of incidents based on its own detection and discovery capabilities identifying the compromise of credentials associated with nationally significant organisations. The NCSC was able to provide guidance to the affected organisations to secure accounts and infrastructure prior to a more serious compromise.

The graphic below represents tactics observed with high levels of confidence in NCSC incidents and investigations. To qualify this, it is not unusual for the NCSC to be unsighted to aspects of a cyber security compromise. The pre-emptive and preventive nature of our MFN® capability means some malicious activity is disrupted before MITRE ATT&CK TTPs can be observed. Our focus on defence and remediation often limits our opportunity to investigate or observe TTPs associated with the latter parts of the compromise. Lastly, not every organisation has tuned their logging capabilities to enable analysis following a possible compromise.

Most recorded MITRE ATT&CK tactics and techniques observed by the NCSC in 2022/2023



For further information about MITRE ATT&CK tactics and their techniques and their specific ID numbers, refer to the MITRE ATT&CK website (attack.mitre.org).

High-impact tactics and mitigations

In the course of the NCSC's 2022/2023 investigations, we identified a number of recurring tactics malicious cyber actors have used effectively in high-impact incidents. A selection of tactics is paired here with steps organisations can take to mitigate the threat. The mitigations below are arranged according to the functions of the NCSC Cyber Security Framework (see page 5 for more information). Many of these mitigations are technical and predominantly aimed at security leaders. However, Guide and Govern statements are intended for non-technical leaders.

Preparation:

Common Vulnerabilities and Exposures (CVEs) – a vector for state and criminal actors alike

Any device on the edge of an organisation's network, no matter how trusted, has the potential to cause disruption or become a vector for a cyber security compromise. The NCSC is aware that state-sponsored and criminally motivated cyber actors alike have regularly scanned for and taken advantage of recently disclosed CVEs, causing disruption or information security concerns for a number of significant Aotearoa New Zealand organisations. In most cases, New Zealanders are not selected as specific targets by malicious cyber actors, but the fact they rely on a vulnerable product or service exposes them to risk. The speed with which malicious cyber actors can mobilise to exploit a vulnerability widely has likely increased year-on-year.

Managing the threat

The main ways organisations can manage the threat presented by CVEs are: having visibility of CVEs, swiftly implementing patches, and checking to confirm whether compromise occurred before patches could be put in place.

- **Identify and Understand:** The NCSC recommends organisations maintain good awareness of CVEs and patches – by monitoring feeds, subscribing to alerts and advisories from CERT NZ, NCSC, and other commercial vendors. Organisations should check and update the list of staff receiving alerts to swiftly identify vulnerabilities and understand whether action is required.
- **Prevent and Protect:** The NCSC recommends organisations seek to reduce the amount of manual patching staff are required to do, and have an expedited patch process for high risk CVEs. Using a two-week test-and-update process for CVEs that are known to be exploited is a high-risk approach, potentially exposing organisations to compromise. Organisations should have an expedited patching process that identifies thresholds for activation, and a streamlined process so patches can be put in place within 48-72 hours.
- **Detect and Contain:** For high-score CVEs, it is not safe to assume a patch was applied before exploitation, even with an expedited process. The NCSC recommends organisations check indicators of compromise (IoCs) to provide confidence that patches were completed before a compromise occurred. The NCSC is aware of multiple cases where an organisation assumed it was secure due to applied patching, but in fact, threat actors had already compromised their systems and gained persistence.

Engagement:

VPN and WFH - vulnerabilities hung over from pandemic pivot

In previous years, the NCSC identified instances of malicious cyber actors exploiting fear and uncertainty generated by the Covid-19 pandemic. This year, the NCSC observed other long-tail consequences of the global pandemic: remote-working architectures established or expanded in haste. A number of NCSC incidents in the 2022/2023 year involved the use of legitimate virtual private network (VPN) credentials. Malicious cyber actors either create privileged accounts after compromise, or harvest credentials on the network or via social deception. Regardless of how malicious cyber actors gain access to legitimate VPN credentials, what is intended to enable flexible working could become a vector for compromise or network persistence.

Managing the threat

Overall, we recommend organisations move towards a zero trust architecture. The concept of having a singular network, or core set of workplaces, has been significantly eroded in recent years. Organisations need to move to focusing on securing identities, devices and data rather than continuing to invest exhaustively in perimeter defence approaches.

- **Guide and Govern:** Leaders should question if their organisations' security training takes into account remote working as part of normal work patterns. Some questions leaders could ask their security team include: Are there better, safer ways for our people to work remotely? Have we reviewed remote working changes we made in 2020 and 2021 for additional security risks to our organisation?
- **Identify and Understand:** Identify any network, architectural and permissions changes the organisation implemented due to Covid-19 lockdowns, and remote-working requirements. Understand the vulnerabilities these changes may have introduced or exacerbated. Do those emergency changes still need to be in place? Make a plan for addressing any new weaknesses. We recommend seeking to implement tools and technologies that support zero trust approaches, such as conditional access, and replacing VPNs with identity-aware web-based proxies.
- **Prevent and Protect:** We recommend endpoint detection and response (EDR) software, rather than anti-virus software, for all organisations. EDR is a critical component of managing devices, and enables not only identity checks, but also device health, as a part of authorising access to organisational information. We recommend multi-factor authentication for remote connections and remote working. Further, following zero trust principles, the types of actions available to a user when working outside the office should be limited in an appropriate way, according to the type of role they have.
- **Detect and Contain:** Malicious cyber actors using remote workers' credentials still need to move laterally across trust boundaries and internal network segregations. Ensuring good logging and alerting on trust boundaries is critical to detecting cyber threat actors if they persist and evade detection.

Persistence:

Disabling security tools - always a reliable indicator for detecting malicious cyber activity

Malicious cyber actors seek to extend their network access through a cluster of techniques known as 'defence evasion'. In a number of significant incidents recorded by the NCSC in the 2022/2023 year, malicious cyber actors disabled inbuilt security controls or deleted activity logs to hide their tracks. The act of disabling endpoint or anti-virus capabilities is in itself a reliable indicator of malicious cyber activity occurring on computer networks.

Managing the threat

- **Guide and Govern:** Some questions leaders could ask their security team include: Do our detection and monitoring approaches cover our cloud environments? Would we know if a threat actor was changing our cloud monitoring alerts?
- **Prevent and Protect:** Only administrators should be able to deactivate security tools. We further recommend organisations require re-authentication, with mandatory multi-factor, in order to turn off any security tools or alerts.
- **Detect and Contain:** Disabling endpoint or network detection tools or rules is itself a high-fidelity security alert. Detection systems, or providers, should treat this as highly suspicious behaviour that always warrants investigation.

Effect:

Legitimate cloud storage providers - an unwitting haven for internet extortion

Several incidents showing indicators of ransomware in the 2022/2023 year involved the use of legitimate cloud providers for data exfiltration. Malicious cyber actors likely prefer these services for extracting large volumes of data quickly and undetected. Cloud storage often features scalable storage and fast, free inbound bandwidth. Connections between Aotearoa New Zealand organisations and large cloud computing or storage providers are not uncommon and may not initially raise alarms.

Managing the threat

- **Guide and Govern:** Some questions leaders could ask their security team include: Do your staff know what cloud storage tools they are supposed to use and are they trained in how to use them? Do staff have formal ways of requesting access to new tools? Does the organisation understand, and account for any cloud-based services you use with your suppliers or customers?
- **Identify and Understand:** Organisations should identify and document the cloud providers they use, and for what purposes. If an organisation has a wide array of cloud services and cloud storage in use, understanding the use cases will help rationalise a manageable number of services. Remember, complexity is the enemy of security.
- **Prevent and Protect:** Blocking cloud services an organisation doesn't use is often not possible. Simply blocking access to unsupported cloud platforms may inadvertently hinder productivity and staff experience, for instance by preventing collaboration between organisations. Instead, we recommend implementing data loss prevention (DLP) processes and technologies. This will help address the core concern: data loss risks.
- **Detect and Contain:** Once an organisation is aware of common cloud services it uses, implementing alerts for connections and heavy outbound traffic will help detect anomalies and unusual behaviour. With DLP in place, have the relevant DLP alerts ingested into a detection solution.

A range of efforts required

In this section the NCSC has provided some key, actionable mitigations for these common threat vectors. The NCSC continues to recommend organisations distribute their security personnel, investment and tools across the five functions of our cyber security framework. Good detection capabilities – paired with protective technologies such as endpoint detection and response (EDR) software – in place across a well-architected environment, with well-enforced trust boundaries, can significantly raise the cost, time and difficulty for cyber threat actors. As well as being a critical Prevent and Protect tool, a quality EDR tool has significant advantages in the event of incident response.

INTERNATIONAL LANDSCAPE

Te āhuatanga i te ao

The NCSC continues to observe a complex international cyber threat landscape with widening access to tooling and knowledge of malicious cyber tradecraft. As governments take action to curb cyber criminal activity, criminal actors become more assertive in their operations in order to achieve their objectives. The international cyber threat environment remains volatile as a result of the Russian invasion of Ukraine in 2022, with an increase in high-profile issue-motivated malicious cyber activity observed in support of both sides of the conflict.

Cyber crime and disruption

The numerous disruptive financially motivated cyber incidents the NCSC recorded this year reflects the international landscape. Significant suppliers were compromised and held to ransom, with the manufacturing and healthcare sectors among the most impacted globally this year. Cyber criminals target these sectors owing to their sensitivity to downtime and disruption, and reliance on older technology.

In past years, the NCSC observed extensive targeting of software vulnerabilities, predominantly from sophisticated cyber actors. Cyber criminals are now capable of this speed and scale of exploitation, previously the purview of likely state-backed actors. This was evident in June 2023 with the re-emergence of 'Clop' ransomware targeting users of Progress Software's MOVEit Transfer, a web based file-transfer application. Clop accessed over 100 instances of MOVEit using a zero-day vulnerability in the software, targeting organisations in the government, manufacturing, media, transport, retail, and professional services sectors. Clop, first observed in 2019, was among the pioneers of the 'double extortion' tactic – exfiltrating sensitive data before encrypting the victim's copy of the files. Increasingly cyber criminals forego the encryption step, preferring to rely on data exfiltration to use as leverage over victims.

While power and popularity has coalesced in the hands of a few dominant ransomware-as-a-service providers over the 2022/2023 year, it has not entirely expunged opportunity for novel variants and new players. Just as we have observed enhanced speed and innovation in the 'initial access' phase, encryption has evolved and become increasingly automated. Cyber criminals have also optimised for the ransom of suppliers. For instance, developing malware to achieve high-impact compromises of hypervisors – an enabling software commonly used by infrastructure-as-a-service providers. Disabling of a hypervisor could have far-reaching impacts for multiple organisations that have a presence on the same physical hardware.

Hypervisior
Software enabling the creation, management and running of discretely hosted virtual machines (VMs) on the same hardware.

Cyber criminals will continue to innovate, whether it is in the area of encryption, deployment, defence evasion, or extortion tactics. In some instances, the perception of encryption is enough to deceive unwitting individuals and organisations, and in others, partial encryption of just a portion of a file has been an effective way to disrupt business processes at pace.

In our region, the NCSC observed significant disruptive malicious cyber activity affecting our Southwest Pacific neighbours. Vanuatu and Tonga had their resilience tested by significant cyber incidents against government and telecommunications systems this year. To aid their recovery, CERT NZ provided advice and support to Pacific victims of profit-motivated disruption.

Investing in and reinforcing resilient practices, along with detecting and responding to incidents in a timely way, are core to deterring cyber criminal activity. However, disruptions to criminal infrastructure and operations is an increasingly common form of deterrence. Collaboration between law enforcement organisations led to seizures of criminal infrastructure in the fiscal year. For instance, the US Federal Bureau of Investigation (FBI) seized infrastructure belonging to Hive ransomware operators in January 2023, announcing it had infiltrated Hive's network since July 2022. In doing so, the FBI was able to provide over 300 decryption keys, negating US$130 million of ransom demands.

In an effort to discourage payments to organised criminals that perpetuate the cyber criminal ecosystem, many likeminded countries are putting in place clear disincentives for paying ransoms, and insurers are increasingly excluding cyber ransom payments from their policies. Also in the 2022/2023 year, Microsoft and Forta (makers of Cobalt Strike, a popular penetration-testing suite) took legal action to identify and disable pirated and legacy instances of Cobalt Strike. Malicious cyber actors commonly abuse Cobalt Strike's capabilities to enable their malicious computer network operations. These kinds of actions have likely set precedent as a novel way to deter cyber criminal activity.

This timeline highlights a range of sectors, impacts and malicious actors in a growing, contested ransomware ecosystem. It also identifies a range of law enforcement disruptions and 'take-downs' that help to curb this malicious activity.

Timeline: A selection of high-impact ransomware events and disruption efforts

August 2022 *Lockbit:* Center Hospital Sud Francilien, France – health records potentially exposed on leak site

US State Department shared an image of suspected Conti member, offering a reward for information about other aliases associated with the ransomware group.

September 2022 *Vice Society:* Los Angeles School District, USA – 500GB of data leaked

Optus, Australia - 11.2 million customers' data stolen

October 2022 CommonSpirit Health, USA – privacy of over 600,000 patients breached, US$150M in losses

November 2022 Vanuatu government, Vanuatu – over a month of disruption, losses included court records

Ransomhouse: Keralty, Columbia – reduced medical services, 3TB lost

December 2022 *Play:* Rackspace, USA – ransomware targeted hosted instances of Microsoft Exchange

January 2023 *Lockbit:* Royal Mail, UK – a ransom of US$80M was demanded but not paid

Hive ransomware infrastructure seized; FBI had infiltrated Hive's network since July 2022 and provided over 300 decryption keys, negating US$130 million of ransom demands.

February 2023 *Lockbit:* Indigo, Canada – impacts to point-of-sale and e-commerce capabilities

Medusa Locker: Tonga Communications Corporation, Tonga – impacts to on-boarding, customer service and billing

Sanctioning of members of Wizard Spider, operators of Trickbot, and with connections to Conti ransomware.

March 2023 Ferrari, Italy – customer details breached

ChipMixer platform seized by German law enforcement (BKA) and the FBI, taking back 7TB of data and US$46.5m in Bitcoin.

Europol disrupted DoppelPaymer ransomware operators, responsible for the University Hospital, Dusseldorf campaign in September 2020.

April 2023 *Money Message:* Micro-Star International, Taiwan – possible key material breached

Seizure of infrastructure hosting Netwire remote access trojan, previously used as first-stage malware in high-quality phishing emails from the cyber criminal group Opera1er.

Microsoft, Fortra, and Health Information Sharing and Analysis Center took legal action to disrupt pirated and legacy copies of customisable penetration-testing suite, Cobalt Strike.

May 2023 *ALPH:* Constellation Software, Canada – finance systems impacted

June 2023 Eisai, Japan – logistics system impacted

Clop: British Airways (UK), Siemens Energy (Germany), Schneider Electric (France), Crown Resorts (Australia), among others

Obfuscation complicating detection

In 2022/2023, cyber security industry reporting identified a number of sophisticated botnets with the primary purpose of obfuscating the true origins of malicious cyber activity. During investigations into PRC malicious cyber activity, partners identified the use of compromised small office/home office (SOHO) devices in the geographic area of the victim.

Over the 2022/2023 year, malicious cyber actors have exploited weaknesses in a number of aging or end-of-life SOHO devices, notably routers and internet modems. SOHO devices are likely preferred for these more sophisticated botnets, owing to their capacity to handle high volumes of network traffic without causing service degradation, thereby avoiding alerting their legitimate users to the compromise.

Botnets almost certainly provide malicious cyber actors with cost-savings, too. For many sophisticated cyber actors, the exploitation of even thousands of vulnerable devices almost certainly falls short of the cost associated with maintaining operational infrastructure via legitimate providers. Additionally, legitimate providers are more likely to have monitoring and complaints processes that could disrupt malicious cyber activity on their platforms.

Industry analysis suggests compromise of internet-connected devices, such as routers or internet-of-things (IoT) devices, could also enable further compromises of inner network devices – previously assumed to be secured behind a gateway.

These internationally identified trends in tactics and techniques for infrastructure procurement corelates with the NCSC's own observations about the compromise of devices for use in botnets over at least the last two fiscal years.

Artificial intelligence has also begun to uplift malicious cyber actors' defence evasion. Large language models and generative AI may be misused to add an air of legitimacy to a phishing campaign – thwarting human defences. Meanwhile, AI can quickly synthesise derivitive malware that could evade technical detection capabilities. In 2022/2023, the NCSC observed rapid advances in AI and early signs of it being used in malicious cyber activity overseas. Big data could also enable the reconnaissance function of a malicious cyber campaign, including surmising connections between disparate pieces of personal or network information, or painting a picture of a victim's preferences, to inform the malicious cyber actor's approach.

It is also likely that AI enables greater cyber defences. AI-derived heuristics may be better than humans at identifying 'living off the land' and other hard to track techniques where a number of innocuous actions need to be assessed together in context to identify activity that is malicious.

Targeting the security supply chain

A feature of the international landscape in 2022/2023 was incidents affecting the security supply chain – software or services relied on to enable information security.

In August 2022, the popular password manager LastPass announced that its proprietary technical information and source code had been breached as part of a cyber incident. Security services represent a valuable target for both espionage and financially motivated actors. It is possible the malicious cyber actors sought an understanding of LastPass' systems and controls in order to stage a more audacious compromise of users' password vaults. These passwords may enable downstream access into networks of high intelligence or extortion value.

In the same month Twilio – a short message service (SMS) provider – reported a compromise during which a small but significant subset of customers was targeted. Accounts targeted belonged to the makers of the secure messaging application Signal, and the two-factor authentication application Authy. This deliberate targeting of specific Twilio customers suggested intent by malicious cyber actors to insert themselves into significant organisations' security supply chains.

A coalescence of security services into the hands of a few cloud-based suppliers has provided security gains and, equally, incentive and opportunities for cyber threat actors. It is likely these high-profile examples have both resulted in a security culture change and uplift at similar organisations, while providing examples and proofs-of-concept to other capable malicious cyber actors.

Information operations

Information operations rely on technology and techniques similar to those used by malicious cyber actors conducting computer network exploitation. While the NCSC does not focus on tracking and responding to information operations, this overlap can make assessing the cyber threat environment more fraught.

Increasingly, technology enables a wider array of information operations. Just as commercial spyware has enabled more states – and even private organisations – to conduct commercial or political espionage, so too have private contractors systematised the spread of information to achieve strategic objectives. In some cases, information operations may be combined with computer network exploitation to meet requirements. For instance, contractors working for political candidates or incumbents to destabilise their opposition may compromise the email or social media accounts of their opponents, as well as manipulating discourse through inauthentic behaviour on public social media platforms.

Information operations

Information operations involve the malicious spread of information to influence or usurp the authority of a victim – usually a nationally significant organisation, politician, or government. Information operations often involve the use of inauthentic behaviour and spread of misinformation via commercial, public technology platforms – such as news websites or social media. They rarely involve the compromise of the confidentiality, integrity or availability of computer networks.

Information collected as part of a malicious cyber campaign might also shape the information environment. Hack-and-leak activity targeting prominent individuals or groups would be a form of malinformation – a truth used to inflict harm on a person, organisation, or state.

The NCSC has a mandate to disrupt and support the victims of malicious cyber activity affecting the confidentialty, integrity or availaiblity of Aotearoa New Zealand nationally significant computer networks. As such, the NCSC has a limited role when it comes to information operations, but we are responsive to reporting from our security partners and the public regarding possible information operations.

Russia-Ukraine

Shifts in the cyber threat landscape following Russia's invasion of Ukraine in February 2022 continue to be felt internationally. Russia-aligned cyber actors are likely emboldened by the invasion, and we continue to see concerning activity affecting Russia's neighbours and our like-minded partners. As the invasion persisted into 2023, malicious cyber activity continued to be observed in support of Russia and Ukraine, albeit not to the extent many suspected. The support Ukraine received to improve their cyber defences may have hampered the effectiveness of Russia's actions in cyberspace.

Whatever the case, Russian malicious cyber activity has likely continued its pre-invasion trajectory, including targeting individuals of high espionage value with sophisticated social engineering and malware. This traditional cyber espionage has been punctuated by disruptive cyber campaigns directed at Ukraine and Russia's other neighbours.

A theme of the year's cyber landscape has been the rise of issue-motivated malicious cyber actors on both sides of the conflict. On the Russian side, these actors are likely emboldened by permissive attitudes to cyber-enabled crime within Russian borders. Issue-motivated cyber activity has usually followed the public commitment of support to Ukraine from Western democracies. Issue-motivated malicious cyber actors have widely targeted Western organisations with denial-of-service campaigns, including in the healthcare sector, with mixed success. The NCSC remains concerned about accidental escalation as a result of disruptive malicious cyber activity stemming from the Russia-Ukraine conflict.

The main cyber threat to Aotearoa New Zealand due to Russia's invasion of Ukraine is indirect cyber targeting, affecting our critical supply chains. State-sponsored and non-state cyber actors alike could disrupt key suppliers on which Aotearoa New Zealand organisations depend.

> "The support Ukraine received to improve their cyber defences may have hampered the effectiveness of Russia's actions in cyberspace."

CONCLUSION

Whakakapi

New Zealanders are digitally connected and globally aware. Aotearoa New Zealand organisations contribute to global knowledge and marketplaces via digital collaboration and connections. Our livelihoods and economy are increasingly dependent on global supply chains and digital connectivity. Whether it is AI content generation, smart cars, or faster communications protocols, companies are investing rapidly in new technology. These emerging conveniences all require an element of information security, or have potential to be disrupted by cyber-borne threats.

Meanwhile, the cyber threat landscape remains volatile. High profile incidents capture the attention of the public and media, and cyber incidents continue to challenge and impose costs on the organisations affected, often for a significant length of time. Cyber criminals continue to find ways to evade defences and inflict costs, even in the face of tightening legislation and combined law enforcement activity. Established approaches to setting and enforcing cyber norms are less reliably dissuading sophisticated cyber actors.

Looking ahead to 2024, it will be important for Aotearoa New Zealand organisations to embed good processes – both in technical controls and in cyber security governance.

In cyberspace, malicious actors are becoming more adept at covering their tracks and circumnavigating traditional defences. We expect this trend to hold in the coming year, with novel botnets, or increasing use of legitimate tools for malicious purposes. The situation in Ukraine may change rapidly, and activity in cyberspace may trigger escalations with significant consequences.

For the NCSC, the coming year will continue to be one of growth and change. As part of this process, we welcome our partners at CERT NZ as colleagues. Our collective strengths will combine to create an even more effective operational agency, ready to respond to the growing cyber security threat faced by people and businesses in Aotearoa New Zealand.

Getting in touch

For general enquiries or to subscribe to NCSC vulnerability alerts: Please email info@ncsc.govt.nz

To see the latest NCSC news, updates and the resources and guides mentioned in this report, visit our website and follow us on LinkedIn:
www.ncsc.govt.nz
www.linkedin.com/company/ncsc-nz/

To report suspicious activity: If your organisation requires assistance, please complete the Cyber Security Incident 'Request for Assistance Form' (www.ncsc.govt.nz/incidents). You can speak with us directly by calling (04) 498 7654. You can also contact us via email at incidents@ncsc.govt.nz

GLOSSARY

Rarangi kupu

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 and self-discovered vulnerabilities.
Botnet / Whatunga Pūwerewere	Normally networks of compromised personal or office devices such as internet modems, personal computers, or network attached storage. Malicious cyber actors use these as infrastructure to send spam, perform denial-of-service activities, or attempt to obfuscate the origins of a malicious cyber campaign.
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.
Cryptocurrency miner / Maina moni whitirangi	Malicious software that co-opts computing resources for generating cryptocurrency. Many digital currencies require the solving of computationally intensive mathematical problems in order to generate digital assets.
Cyberspace / Āteatāurungi	The global network of interdependent information technology infrastructures, telecommunication networks, and computer processing systems in which online communication takes place.
Cyber security / Whakahaumaru ā ipurangi	Measures to protect systems, data, and devices from unauthorised access, and ensuring the confidentiality, integrity, and availability of information.

TERM / KUPU	DEFINITION / WHAKAMĀRAMATANGA
Data breach / Raraunga wāwāhi	The intentional or unintentional release of sensitive or private information into an unsecure environment.
Defence evasion / Karo kaupare	A tactic that describes a series of attempts to avoid network defenders discovering a malicious actor.
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.
Disinformation / Ngā kōrero horihori	The deliberate, intentional spread of false and misleading information designed to achieve a strategic purpose.
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.
Hybrid threat / Tuma momorua	A mix of military, non-military, covert and overt activities by state- and non-state-sponsored actors that occur below the line of conventional warfare.
Hypervisor / Kaiwhakahaere pūrere mariko	Software enabling the creation, management, and running of discretely hosted virtual machines (VMs) on the same hardware.
Incident / Maiki	An occurrence or activity that appears to have degraded the confidentiality, integrity, or availability of a data system or network.
Indicators of compromise (IoCs) / Paetohu whakamōrearea (ngā IoC)	Usually IP addresses, domain names, or files that may be shared publicly or in confidence. Together they suggest a computer system or network may be compromised.
Living off the land / He ora nō te whenua	A technique using legitimate and pre-existing software on a victim network, in contrast to the installation of malicious software, to maintain network accesses. Use of legitimate software and accounts is less likely to raise alerts for defenders.
Malicious cyber actor / Nanakia tūkino mōhiohio	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 / Pūmanawa kino	Malicious software or code intended to have an adverse impact on organisations or individuals' data, such as viruses, Trojans, or worms.
Mitigation / Ārai mōrea	Steps that organisations and individuals can take to minimise and address cyber security risks.
Nationally significant organisation / Whakahaere hira ā-Motu	Organisations such as government agencies, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. If these organisations were affected by a cyber security incident, the impact could lead to national-level harm.
Opportunistic cyber activity / Ngohe ā-ipurangi tūpono	Occurs when malicious cyber actors select their victims based on the availability of a vector of compromise, regardless of victim location, sector, or intelligence value.
Personal information / Ngā mōhiohio whaiaro	Information about an individual, including name, date of birth, biometric records, medical, educational, financial, and employment information.
Phishing / Hītinihanga	The use of fake, deceptive, or alluring messages to solicit a behaviour from the recipient – such as clicking a link or divulging personal information or credentials.
Public attribution / Whakahuatia whānuitia nō hea	A tool used by governments and private sector organisations to deliberately release information about the source of a cyber intrusion, primarily to uphold norms about what constitutes acceptable state behaviour in cyberspace.
Ransomware / Pūmanawa utu uruhi	A type of malware designed to disrupt the use of computer systems and files until a ransom is paid.
Supply chain compromise / Poke ara ratonga	A form of attack that targets software, hardware, or an IT service provider, where the ultimate aim is to exploit downstream customers.
Targeted cyber activity / Ngohe ā-ipurangi heipū	Occurs when malicious cyber actors demonstrate an intent or a tasking to compromise an organisation for its intelligence value, regardless of a specific access vector.
Virtual private server (VPS) / Tūmau tūmataiti mariko	A portion of a large physical server divided into virtual spaces available for temporary use.
Zero-day vulnerability / Whakaraeraetanga rā-kore	A software vulnerability for which there is currently no patch, and for which there is often no CVE number assigned. The term derives from the number of days for which defenders and developers have been aware of the vulnerability.

Te Tira Tiaki
Government Communications
Security Bureau

National Cyber
Security Centre