New Zealand Government

New Zealand's cyber security strategy 2019

Enabling New Zealand to thrive online

Published by the Department of the Prime Minister and Cabinet (DPMC), July 2019.
dpmc.govt.nz • information@dpmc.govt.nz

ISBN 978-0-947520-12-0 (print)

ISBN 978-0-947520-11-3 (online)

Ministerial foreword

Cyber security is fundamental to a robust and thriving society

Being connected online has greatly benefited New Zealand and New Zealanders. We are more closely connected to global culture and the international economy than ever before. Internet connectivity brings New Zealand to the world, underpins our prosperity, and helps to negate the downsides of distance.

New Zealanders can enjoy the benefits of this connectedness in their homes and neighbourhoods, and this connectedness is increasingly important to individuals and communities.

The benefits of these global connections will continue to increase. Being able to work, play and interact safely online is a critical enabler for our economic, social and cultural development – New Zealand is becoming a digital nation.

As the benefits increase, so does our dependence on a free, open and secure internet and trusted underlying infrastructure and technology. Almost every aspect of our daily life now depends on the internet and information technology. This ranges from the basic functioning of New Zealand's economy and society – from our jobs, banks, schools – to the delivery of government and telecommunications, and electricity services. While around 90% of New Zealand's population are active internet users, everyone depends on the internet.

Our children communicate with us and their peers online, and their schools use internet as a vital tool. We remain close to friends at a distance and whānau online, we share our news, consume our news and shop online. Importantly, many communities are now internet enabled: these ongoing connections are increasingly vital in our lives.

We need to know that our systems will keep running, that our personal and commercial information is safe, and that we can trust the information that we use to make decisions.

Good cyber security is therefore essential. Cyber security is not simply an IT issue – it's critical for every business and for every person living, working or visiting New Zealand. New Zealand's cyber security policy is therefore about making the most of the opportunities that the internet provides and protecting the things most important to us.

But with new opportunities come evolving cyber security risks. Artificial intelligence (AI) and cognitive technologies are becoming increasingly commonplace, along with a range of internet-connected everyday devices. The arrival of 5G wireless networks is close and quantum computing is on the horizon.

These new technologies will be disruptive. That will allow us to innovate, but may also expose us to greater risk. These technological changes are not happening in a vacuum: the geopolitical picture has also shifted, with a greater range of state actors making the most of cyber-enabled tools to steal information, spread disinformation and launch attacks. New Zealand's response to the evolving risk needs to be commensurate with our dependence on internet connectivity.

This strategy emphasises that the government needs to work with individuals, businesses, community organisations and the private sector, in order to minimise harm and disruption, and make the most of technological advances.

I look forward to working with you all to achieve our vision of New Zealand being confident and secure in the digital world – enabling New Zealand and all New Zealanders – to thrive online.

Hon Kris Faafoi
Minister of Broadcasting, Communications and Digital Media

Challenges to maintaining cyber security

Cyber-enabled threats to our security continue to grow in number, scope and scale. Cyber criminals and malicious state-backed actors are targeting New Zealand now. Access is being sought to our personal information, bank accounts, intellectual property and nationally important data on a 24/7 basis. From home-users to businesses, to government to critical national infrastructure, everyone using the internet faces a constant and evolving threat. Potential harms include financial losses, reputational damage, loss of intellectual property and disruption to critical services. Constant vigilance and active protection of our sensitive data and networks is no longer optional. We also need to be ready to detect, respond to, and recover from any intrusions.

Technology is evolving quickly...

The nature and consequences of cyber incidents can vary widely, and, as new technologies are developed and adopted, new threats will emerge. Responding to these threats in the context of rapid technological change will require us to adapt quickly. The exponential increase in the use of IoT (Internet of Things) devices is an example of how the rush to deploy new products and services has led to the re-emergence of security issues that had been largely addressed in mature technology sectors. In October 2016, millions of IoT devices were taken over to form the Mirai botnet, which was used to launch a massive denial of service attack that disrupted the internet for almost the entire eastern United States.

Cyber security is a complex problem – it's about people, policies, technology, trust and reliability. It is not always possible to predict what will happen and at what pace.

The emergence of AI is an example of a technological shift where the impact for cyber security is largely unknown. The potential national security issues posed by the adoption of 5G technology present new and different risks from that of previous generations of mobile infrastructure. Cyber attacks can also have unintended consequences: the NotPetya malware* initially only targeted Ukrainian entities but ended up spreading to cause damage and disruption across the globe.

...And threat actors are on the increase and becoming more sophisticated...

The number of malicious actors seeking to do harm on the internet also continues to rise. Threat actors of all kinds are increasingly bold, brazen and disruptive. As more people use and do business on the internet, the pay-offs from cyber and cyber-enabled crimes will also increase, attracting greater numbers of cybercriminals. Almost every cyber attack is a criminal act, regardless of who is behind it.

Cyber criminals and other threat actors are becoming more sophisticated. More and more, threat actors from individuals to nation states have access to the same tools and techniques. In 2017, the WannaCry outbreak caused major international disruption, including shutting down computers in the United Kingdom's National Health Service. WannaCry was attributed to North Korean actors by a number of New Zealand's international partners, highlighting how nation states can use cybercriminal tools, and vice versa.

* NotPetya malware: a particular piece of malicious software that spread across the internet and encrypted (locked up) files on an infected computer system. A number of states have attributed this malware to Russian state actors.

Cyber risks are growing in an increasingly contested international order. In the context of growing great power competition and increasing challenges to the international rules-based order, state-sponsored actors are using cyber tools for geopolitical advantage. The number of state-sponsored cyber operations is rising and more governments are openly developing offensive cyber capabilities. Cyber tools have been used by state-sponsored actors to steal sensitive commercial information, to disrupt critical systems and to interfere with democratic processes.

...So New Zealand must be ready to deter and respond to threats

New Zealand must stand up for responsible state behaviour in cyberspace, and advocate for an international rules-based order that promotes a stable and peaceful online environment. New Zealand must also be ready to deter and respond to cyber threats when they arise.

As all nations improve their cyber security, and where users respond to one cyber security challenge, malicious actors will seek new vulnerabilities and opportunities. New Zealand must stay towards the front of the pack so that it does not become a target of choice – we want to erect barriers against malicious actors.

There is no simple way to articulate the cyber security risk to New Zealand, because the threats are so diverse. The challenges for home-users are not necessarily the same challenges that our largest companies face. But it is clear that trust and confidence in the internet and our internet infrastructure is vital for New Zealand and New Zealanders: for our economy, for our society, and for our national security. We all need to take action to maintain that trust.

Case study: WannaCry

WannaCry ransomware spread across the globe in May 2017 in one of the most disruptive cyber attacks to date.

Ransomware is a kind of malicious software that locks up the files on a computer system until a sum of money is paid.

WannaCry affected over 200,000 computers in at least 100 countries. The United Kingdom's National Health Service was particularly badly affected, with systems down in hospitals across the United Kingdom, forcing the cancellation of nearly 20,000 hospital appointments.

The attack also affected major companies, including French car manufacturer Renault and international shipping company FedEX.

In December 2017, New Zealand publicly highlighted its close partners' attribution of the attack to North Korea. The United States has subsequently charged a North Korean hacker in connection with this attack.

What have we done so far?

New Zealand has issued two previous cyber security strategies in response to this challenge. The 2011 strategy outlined the Government's response to the growing threat and established the National Cyber Security Centre and the National Cyber Policy Office. The 2015 Cyber Security Strategy acknowledged that technology was transforming New Zealand and outlined a vision of a secure, resilient and prosperous online New Zealand.

Since 2015, a range of actions have been taken to advance that vision, including the establishment of CERT NZ to respond to cyber security threats in New Zealand, New Zealand's first Cyber Security Summit, the Government Communication Security Bureau's (GCSB) deployment of CORTEX services to nationally significant organisations (preventing $67 million of financial harm in the first 2 years of operation), GCSB's development of Malware-Free Networks, the designation of the Director-General of the GCSB as the Government Chief Information Security Officer, the introduction of greater cybercrime training for New Zealand Police, and the development of a cyber credentials scheme to help small businesses improve their cyber security.

But the world has shifted since 2015 and our response has to adapt to these changes.

Social engineering is one of the most commonly used techniques among cyber criminals.

For example, in a recent case, an employee of a finance company was deceived into providing credentials, after responding to a phone call from a person claiming to be from the helpdesk. The criminal then used the employee's login details and emailed the company's customers, asking them to pay invoices from the company to the criminal's bank account instead. Several customers did so before the breach was uncovered. The account was closed down, but not before several customers had paid a total amount in the $100,000s.

In cases like this, no one "hacked" into the company's network – they breached the company's security by tricking the employee. The employee lacked cyber security training, and were unaware of the threats and the measures needed to protect themselves and their company from this kind of crime.

Cyber threats by the numbers

CERT NZ 2018 Summary Report

CERT NZ supports businesses, organisations and individuals affected by cyber security incidents

3445 incidents reported in 2018

OVER
$14.1m
in total financial loss

Most reported incidents:
phishing and credential harvesting
(stealing people's IDs and passwords)

National Cyber Security Centre: Cyber Threat Report 2017–2018

The NCSC helps New Zealand's most significant public and private sector organisations protect themselves

39% of those incidents linked to state-sponsored actors

What does this mean for New Zealand?

New Zealanders and their businesses are losing money every day.

People's accounts and personal data are being compromised.

State-sponsored actors are targeting organisations that are significant to New Zealand.

Our vision

New Zealand is confident and secure in the digital world: Enabling New Zealand to thrive online

This strategy has a vision that New Zealand is confident and secure in the digital world – it is about enabling New Zealand to thrive online. We want New Zealanders to make the most of the opportunities provided by an increasingly connected world, without suffering harm or loss. The vision acknowledges that while connectivity brings risks, we can take action to minimise those risks, and that connectivity has become vital for New Zealand's society and economy.

It is an opportunity for the New Zealand Government to take a lead in responding to cyber risks but also for us to achieve this vision as a nation. One of the priority areas in this strategy is to develop cyber security aware and active citizens. There are actions we can take collectively to reduce the risk for everyone, and responding to emerging issues requires everyone to take action: individuals, businesses, non-government organisations, and government. This strategy outlines the areas in which we will prioritise action and how we will work together.

Guiding principles

This strategy sets out five priority areas for action to deliver the vision. To deepen collaboration and to take effective collective action in each of these areas, we will work in a way that:

- builds and maintains trust
- is people-centric, respectful, and inclusive
- balances risk with being agile and adaptive
- uses our collective strengths to deliver better results and outcomes
- is open and accountable.

These principles are a practical way of giving effect to the values that underpin the strategy and to get more effective results.

These principles acknowledge that cyber security is not a 'problem' the government can fix, it is everybody's responsibility and means we need to work together in different ways to get better results. These principles were designed using feedback from the engagement as the strategy developed.

Our values

This strategy signals the Government's commitment to enabling New Zealand and New Zealanders to thrive online. But we can only achieve that if we work together. New Zealand's small scale and relatively simple telecommunications and network structure enables the public and private sector to work closely together to embed a cyber security culture, and to respond to evolving cyber risks.

New Zealand is a modern, progressive, safe and internationally-collaborative country. Our cyber-security system is maturing. New institutions like CERT NZ have been established and all our government agencies with cyber security responsibilities are building significant connections across the system, both domestically and internationally.

Partnerships are crucial

The government has a leadership role to play in cyber security – but not on its own. Close partnerships are required with the private sector, non-government organisations and the international community. Businesses drive the New Zealand economy and depend on the internet and networked technologies. They must protect the information that is critical to their commercial success. The private sector and technical community have considerable cyber security expertise, and we need to work with international partners in order to combat trans-national threats.

People are secure and human rights are respected online

The openness of the internet is part of its unique value – allowing for unrestricted participation and the free flow of information. People need to be able to operate in the digital world confident that their privacy will be protected and that their private and financial details will be protected. They should be able to engage online without suffering harm or unlawful interference, and be able to pursue criminal and consumer redress when things go wrong.

Human rights should be protected online as they are offline. International and domestic law similarly apply online as offline. This includes the right to freedom of expression, and the protection of privacy, as set out in New Zealand law and existing international law.

Economic growth is enhanced

Strong cyber security practices result in businesses remaining productive, profitable and transparent to customers and shareholders. New Zealand will be recognised as a desirable place to do business, store data, and invest. Information and communication technologies and enhanced connectivity will continue to boost economic growth, and minimise costs of cyber insecurity. New Zealand and New Zealand businesses can benefit from the growth of the digital economy and new technologies can help drive innovation.

National security is protected

Cyber threats to New Zealand – particularly state-sponsored espionage, cyber terrorism, theft of intellectual property from government and critical infrastructures – are national security risks. Upholding New Zealand's national security in the face of this threat is a fundamental part of a successful strategy. Protecting our national security requires us to be adaptable, resilient, and prepared to manage uncertainty.

Delivering the vision

Our five priority areas to improve cyber security (2019–2023)

The following sections provide an overview of the five priority areas for this strategy and the actions that we will take to improve New Zealand's cyber security, allowing us to make the most of the digital world.

The cyber security landscape will continue to change with new technologies, risks and opportunities emerging. Predicting the future will not get easier, so our ability and willingness to adapt to change and collaborate is critical.

An annual work programme will accompany the strategy. The work programme will outline a range of actions to advance each of these priority areas. The responsible Minister will release a public annual report on progress under each of the priority areas.

Cyber security aware and active citizens

Strong and capable cyber security workforce and ecosystem

Internationally active

Resilient and responsive New Zealand

Proactively tackle cybercrime

Cyber security aware and active citizens

This priority area is about building a culture in which people can operate securely online and know what to do if something goes wrong. Our work in this area will focus on:

- practical, targeted and regular awareness campaigns to build awareness and resilience among different groups of people
- making it easier for everybody to report cyber incidents and get help from relevant government agencies
- increasing the availability of educative tools so people can be secure and safe online
- increasing efforts to educate vulnerable users, such as the elderly and children, to prevent victimisation
- sharing research so people can understand the threat and vulnerability landscape for their businesses, communities and families.

Strong and capable cyber security workforce and ecosystem

New Zealand needs to be able to rely on a strong cyber security workforce, capable of preventing, adapting to, and responding to threats. Our work in this area will focus on:

- incentivising and increasing the supply of skilled cyber security workers
- supporting the expansion of roles and opportunities for cyber security workers
- incentivising the growth of the cyber security industry in New Zealand
- supporting industry and professional organisations to promote responsible management of cyber security across their organisations and workplaces
- encouraging the development of a world-class cyber security academic research community
- supporting high-quality cyber security research and encouraging links between academia and industry.

Internationally active

New Zealand's interests will be advanced and protected through our international activity. We will continue to champion a free, open, secure internet. New Zealand's voice in international discussions related to cyber issues will support the international rules-based order and promote peace and stability in cyberspace.

New Zealand considers that existing international law applies online as it does offline and supports the development and implementation of norms for responsible state behaviour to maintain a peaceful and stable online environment. Cooperation and dialogue on cyber issues is central to building confidence and understanding to reduce the risk of conflict. We will act bilaterally, regionally and globally to build trust in cyberspace.

We will respond to unacceptable behaviour in cyberspace and we will cooperate with others to prevent and deter malicious activity that threatens peace and security.

New Zealand's international engagement on cyber security issues will:

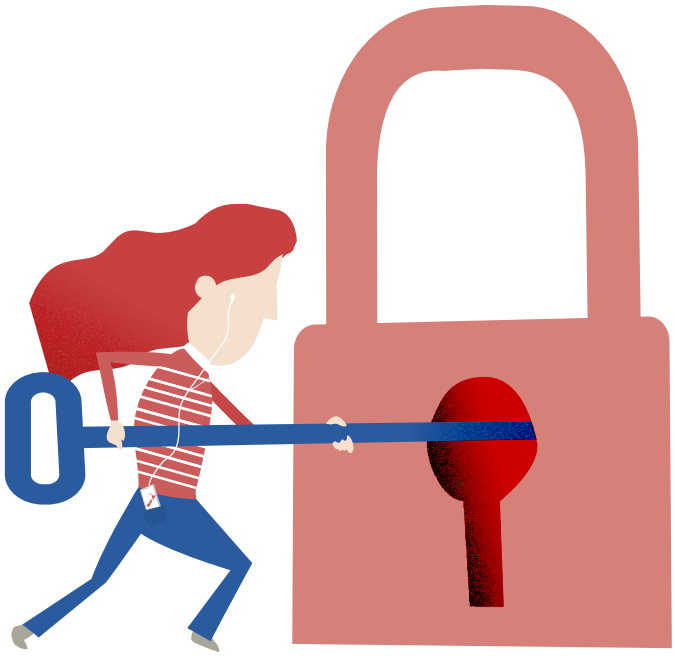
- build clearly prioritised international partnerships and cooperation at policy and operational levels
- influence to support the rules-based international order and a free, open, multi-stakeholder internet
- prevent, detect, deter, and respond to malicious behaviour online
- secure our neighbourhood by strengthening regional capacity-building, confidence, and operational cooperation, including for law enforcement activities
- contribute to New Zealand's economic prosperity.

Resilient and responsive New Zealand

This priority area is about ensuring that New Zealand can resist cyber threats and that we have the tools and know-how to protect ourselves. The focus of this area is expanding from building resilience in significant infrastructure to being able to respond to incidents across the system.

That wider system focus will include:

- vigorously protecting New Zealand's most important information infrastructures
- supporting businesses, NGOs, community organisations, and individuals to be protected and resilient to major cyber incidents
- using cyber tools and partnerships to further New Zealand's interests, including national security and law enforcement activities
- supporting critical national infrastructure organisations and ensuring those organisations take responsibility for the security of their systems
- improving the information security capabilities and resilience of the public sector.



Proactively tackle cybercrime

Criminal activity will continue to adapt and the consequences will become more severe. Our response needs to meet this challenge. New Zealand must proactively and collaboratively prevent, investigate, deter and respond to cybercrime, cyber-enabled crime and terrorist use of the internet. Work continues on implementing the 2015 National Plan to Address Cybercrime, including consideration of accession to the Council of Europe Convention on Cybercrime (the Budapest Convention). We will also continue to work with others on issues related to encryption: ensuring that law enforcement can access the information it needs while balancing the rights of New Zealanders to protect their privacy and security.

Any action to address online harms, such as the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online, will be consistent with New Zealand's wider cyber policy positions, including the importance of maintaining a free, open and secure internet and the application of international human rights law online.

Key areas of focus will include

- seeking Cabinet agreement to accede to the Budapest Convention
- preventing cybercrime particularly for vulnerable groups
- increasing support to people affected by cybercrime
- encouraging reporting of cybercrime and improving sharing of information about cybercrimes
- improving information-sharing between law enforcement and the financial sector to reduce victimisation
- making the law fit-for-purpose to enable agencies to better manage and respond to cybercrime
- investing more to contribute to international efforts to deter organised cybercrime at the source, before it affects our communities
- raising our ability to respond to objectionable material and terrorist activity online
- investing more in skilled people and resources to combat cybercrime and cyber-enabled crime.

Glossary

5G technology
5G is the 5th generation of mobile technology. It is likely to bring higher rates of data transmission, reliability, and connectivity.

Artificial intelligence
A computerised system capable of simulating human decision making and learning, including performing cognitive functions associated with the human mind including learning and language.

Credential harvesting
Collecting legitimate users' usernames and passwords to gain access to target systems, for malicious purposes.

Critical infrastructure/critical national infrastructure
Physical and digital assets, services, and supply chains, the disruption (loss, compromise) of which would severely impact the maintenance of national security, public safety, fundamental rights, and well-being of all New Zealanders.

Cyber attack
Deliberate exploitation of information systems to cause harm.

Cyber incident
An event, whether intentional or not, that causes adverse consequences to an information system or its data.

Cyber security
Protecting people and their computers, networks, programs and data from unauthorised access, exploitation, or modification.

Cyber terrorism
The use of computer systems in committing a terrorist act.

Cybercrime
Crimes that are committed through the use of computer systems, and are directed at computer systems. Examples include producing malicious software, denial of service attacks, and phishing.

Cyber-enabled crime
Crimes that are assisted, facilitated or escalated in scale by the use of technology. Examples are cyber-enabled fraud and the online distribution of child exploitation material.

Cyberspace
The internet and everything connected to it – the global network of interdependent information systems, telecommunications networks and information technology infrastructures.

Distributed Denial of Service Attack (DDoS)
A cyber attack that stops users from accessing a service or resource, by overloading that service with requests.

Encryption
The transformation of otherwise readable data into a form that conceals its original meaning, to prevent it from being known or used. Strong encryption is a fundamental element of good cyber security, which is increasingly critical to New Zealand's national security and economic prosperity.

Information system/computer system
A computer system for the collection, organization, storage and communication of information.

Internet of Things
Computing devices connected to the internet and embedded into everyday objects, enabling them to send and receive data.

Malicious software/ malware
Software designed to infiltrate or damage a computer system. Examples include computer viruses, worms, Trojans, spyware, and adware.

Phishing
Using fraudulent emails to persuade people to reveal confidential information, such as login or banking information.

Quantum Computing
Whereas a classical computer works with ones and zeros, quantum computers have the advantage of using ones, zeros and "superpositions" of ones and zeros. This means they can perform calculations at a far greater rate than classical computers.

Ransomware
A type of malicious software that locks up the files on an information system until a ransom is paid.

Software
The programs used by a computer, as well as other information that it relies on to operate.

New Zealand Government

Published by the Department of the Prime Minister and Cabinet (DPMC), July 2019.
dpmc.govt.nz • information@dpmc.govt.nz