NEW ZEALAND'S CYBER SECURITY STRATEGY

June 2011

New Zealand Government

7 June 2011
ISBN: 978-0-478-38200-6
www.med.govt.nz/cyberstrategy

Foreword from the Minister

The Internet and digital technologies are transforming the global economy and connecting people as never before. New Zealand citizens, businesses and the Government are readily embracing the many advantages that these technologies offer.

Everyday activities such as banking, shopping and accessing government services are increasingly being carried out online whenever and wherever it is convenient for people to do so. New Zealand businesses are using the Internet and other digital technologies to access new markets, drive process efficiencies and improve their service delivery.

The Government's Ultra-Fast Broadband and Rural Broadband initiatives will help New Zealanders maximise the benefits of the Internet by providing significantly faster broadband.

At the same time, our increasing use of the Internet and other digital technologies increases our vulnerability to cyber threats. Criminals are increasingly using cyber space to gain access to personal information, steal businesses' intellectual property, and gain knowledge of sensitive government-held information for financial or political gain or other malicious purposes. National borders present no barrier.

New Zealand's Cyber Security Strategy is the Government's response to the growing cyber threat. The Strategy builds on existing government and non-government efforts to improve New Zealand's cyber security. It brings forward targeted initiatives aimed at improving cyber security for individuals, businesses, critical national infrastructure and government.

The Strategy reflects the fact that an improved New Zealand cyber security response is a shared responsibility. Government will continue to partner with industry and non-government organisations to ensure the initiatives outlined in the Strategy are delivered in the most effective and efficient way.

Meeting the evolving cyber threat requires ongoing vigilance and flexibility to respond to the changing environment. I am confident we can work together to meet this challenge.

Hon Steven Joyce
Minister for Communications and Information Technology

Introduction

A well-functioning cyber space provides important benefits for New Zealanders. The Internet and digital technologies enable New Zealanders to have global access to products and services and reduce our geographical isolation by connecting us with the rest of the world.

Access to greater internet bandwidth and wireless technology – in particular mobile devices such as smart phones – is transforming how New Zealanders access the Internet and how business is transacted in New Zealand. Convenient, high-speed access to information and services is increasingly in demand.

Our critical national infrastructure providers, including the banking and finance, telecommunications, transportation and energy sectors, and other businesses, are more and more reliant on digital systems.

Government agencies utilise the Internet, digital document management systems and shared online platforms in their day-to-day business. Increasingly, New Zealanders are accessing government services online, to complete tasks such as submitting tax returns and making applications for passport renewals and student loans.

Internet Usage

- At least 75% of New Zealanders have access to the Internet at home.[1]
- Over 70% of New Zealand Internet subscribers have access to broadband.[2]
- 77% of New Zealand businesses use Internet banking and 50% of rural businesses buy goods and services online.[3]

With our ever-increasing use of, and reliance on, the Internet and digital technologies comes increased exposure, and vulnerability, to cyber threats.

Cyber attacks are becoming more advanced and sophisticated. Incidents reported internationally suggest that attacks are increasingly targeted at intellectual property and other proprietary information held by businesses, as well as at individuals. Many attackers are coordinated, well-funded, and investing heavily in new ways to exploit the digital environment.

[1] Statistics New Zealand Household Use of ICT Survey – 2009.
[2] *As above.*
[3] MYOB Business Monitor Internet survey – 2011.

An Increasing and Evolving Global Threat

- In 2010 alone, one third of all malware in existence was developed.[4]
- 2010 has been marked by some of the most high-profile, targeted attacks that the cyber industry has ever witnessed.[5]
- There was an upward trend in Trojan botnet activity during 2010, which has gained momentum despite increasing coordinated efforts to shut down botnet activity.[6]
- "Spear phishing", a more targeted phishing technique using information gained from other sources to give a veneer of authenticity, grew in prevalence in 2010.[7]

The Role of Government

New Zealand is not immune from cyber attacks. A successful targeted cyber attack could disrupt our critical services, negatively impact our economy and, potentially, threaten our national security. Cyber attacks can interfere with the production and delivery of essential goods and services or result in the theft of intellectual property or personal information.

New Zealand's cyber security response must meet the challenging nature of the increasing and evolving cyber security threat. New Zealand needs to ensure its cyber security activities are as coordinated and effective as possible to be able to identify and mitigate emerging cyber threats.

The Government has a responsibility to protect its own systems and assist critical national infrastructure providers to ensure New Zealanders and New Zealand businesses can access government and other essential services.

The Government also has a role in helping to provide a safe digital environment for businesses and individuals to operate in. This includes helping New Zealanders and businesses to be more aware of cyber threats, and how to take measures to protect themselves, and establishing appropriate organisational and legal frameworks.

Government units have already been established to tackle issues such as scams, spam, identity theft, electronic crime and critical national infrastructure protection. The Government also provides support to *NetSafe*, an independent non-profit organisation, to deliver cyber safety education and awareness programmes in schools.

The Government is actively working with New Zealand's international security partners on cyber security issues and is currently reviewing New Zealand's legal framework in relation to the growing issue of international cyber crime.

[4] PandaLabs Annual Security Report – 2010.
[5] IBM X-Force Trend and Risk Report – 2010.
[6] *As above.*
[7] *As above.*

Cyber Security Threats

The threat to New Zealanders and the New Zealand economy from cyber intrusions is real and growing.

New Zealanders are already targets of common cyber threats, such as malware, scams and identity theft.

Attackers exploit vulnerabilities in software, hardware and user behaviour. They take advantage of people who fail to follow basic cyber security practices, such as regularly updating their passwords, updating their antivirus software and using protected wireless networks.

Once attackers have access to a computer or network, they can steal or distort the information stored on it, corrupt its operations or program it to attack other computers and systems.

Unprotected home computers that are infected with malware can be used as a resource to build botnets. Botnets harness the computing power of thousands or even millions of individual computers to launch remote attacks on information and communications networks, commercial systems and government websites with the aim of denying the legitimate use of the service.

The Threat to New Zealand

- 70% of New Zealand adults have been the targets of some form of cyber crime[8], with the most common complaints being computer scams, fraud and viruses/malware.[9]
- New Zealanders are frequently the targets of international scams and fraud attempts, losing up to $500 million due to scams annually.[10]
- International data suggests 133,000 New Zealanders per annum are victims of identity fraud (the majority of cases having a cyber element), with around one third falling victim to identity theft and two thirds falling victim to credit or bank card fraud.[11]
- A recent survey showed that 54% of New Zealanders feel they know little or nothing at all about computer security risks and solutions.[12]
- 59% of New Zealanders do not secure their mobile phones, PDAs or smart phones by using, and regularly changing, a password or PIN.[13]

[8] Norton Cybercrime Report 2010: The Human Impact.
[9] New Zealand Police – 2011.
[10] Ministry of Consumer Affairs – 2010.
[11] Department of Internal Affairs – 2010.
[12] AVG/NetSafe Survey – March 2011.
[13] Unisys Security Index – 2010.

Cyber crime

Criminals operating in cyber space are often well-organised and well-funded. They are constantly targeting home users, businesses and government systems. Organised criminals are involved in activities such as identity theft, selling fake goods and services and trading information with other criminals such as stolen credit card details, passwords and malware.

Criminals are finding increasingly sophisticated ways to gain access to information online. For example, as the popularity of social networking sites increases, criminals are exploiting opportunities to use these sites to access individuals' personal information[14]. In addition to obtaining personal information, cyber criminals also seek to obtain intellectual property and government-held information for financial gain.

Social Networking Targets

- Cyber criminals are increasingly using social networking sites to lure victims to websites that attempt to push malware or launch an attack on the victim's computer.[15]
- Attackers exploit the profile information available on social networking sites (e.g. birth dates, phone numbers, employment details and other information) to mount targeted attacks.[16]

Cyber Espionage

Some of the most advanced and persistent cyber attacks on governments and critical infrastructure worldwide are thought to originate from foreign military and intelligence services or organised criminal groups. Media organisations around the world are reporting attacks on government systems, national infrastructure and businesses that have resulted in access to commercially sensitive information, intellectual property and state or trade secrets.

Hacktivism

There has also been a global increase in 'hactivism'. Hacktivists seek to gain control over computer systems or websites to manipulate them to promote a cause, make a political statement or disrupt services, for example, by overloading websites with botnet attacks, which can deny or prevent the legitimate use of the service.

Terrorist use of the Internet

Terrorists recognise the growing worldwide dependence on cyber systems and may seek to take advantage of the vulnerabilities that exist. It is likely that terrorists will continue to develop their cyber capability and use of the Internet to support recruitment and fundraising activities.

[14] Sophos Security Treat Report – 2010.
[15] Symantec Internet Security Threat Report: Trends for 2010.
[16] *As above.*

New Zealand's Response

New Zealand's Cyber Security Strategy outlines the Government's response to the growing cyber threat. The Strategy highlights initiatives for individuals, businesses and government to strengthen New Zealand's cyber security position.

The key objectives of the Strategy are to:

- raise the cyber security awareness and understanding of individuals and small businesses;
- improve the level of cyber security across government; and
- build strategic relationships to improve cyber security for critical national infrastructure and other businesses.

The Government has appointed the Ministry of Economic Development as the lead policy agency responsible for coordinating cyber security policy and implementing this Strategy.

A Partnership Approach

Improving cyber security is a shared responsibility. In developing this Strategy, the Government has sought input from a wide range of stakeholders across government, industry, non-government organisations and academia.

The Government will continue to build partnerships and work with these stakeholders to implement the initiatives outlined in the Strategy and to explore further opportunities to enhance New Zealand's cyber security response.

Internationally, the Government will continue to collaborate with security and trade partners to ensure New Zealand contributes effectively to global cyber security initiatives.

Priority Areas and Key Initiatives

New Zealand's Cyber Security Strategy has three priority areas:

1. Increasing Awareness and Online Security
2. Protecting Government Systems and Information
3. Incident Response and Planning

The Strategy identifies key initiatives, and longer-term initiatives, under these priority areas. Implementation of the key initiatives will begin in 2011.

Priority 1 – Increasing Awareness and Online Security

Individuals and businesses have a responsibility and interest to ensure they carry out their activities in cyber space as safely as possible. The Government has a role in helping to enable a safe cyber environment and helping New Zealanders and businesses to access the tools and information they need to operate as securely as possible in cyber space.

The Government is working with industry and non-government organisations, such as *NetSafe*, on initiatives to improve access to cyber security information and advice. The Government is also working with industry and non-government organisations on initiatives to raise the cyber security awareness of individuals and small businesses and to increase understanding of cyber security threats.

The Government will seek the views of Internet Service Providers and other organisations on measures to address problems such as infected computers and botnets.

Key initiatives:

- Partner with industry and non-government organisations, such as *NetSafe,* to:
  - centralise cyber security information and resources for ease of access; and
  - deliver a coordinated cyber safety awareness-raising programme.

Longer-term initiative:

- Progress work with Internet Service Providers to develop appropriate solutions to address cyber security issues, such as infected computers and botnets.

Priority 2 – Protecting Government Systems and Information

The Government has a responsibility to protect the personal and commercial information entrusted to it by its citizens and businesses from harmful or unauthorised use. Nationally sensitive material must also be protected.

As a priority, the Government will establish a National Cyber Security Centre within the Government Communications Security Bureau.

The National Cyber Security Centre will build on existing cyber security and information assurance capabilities to provide enhanced protection of government systems and information against advanced and persistent threats.

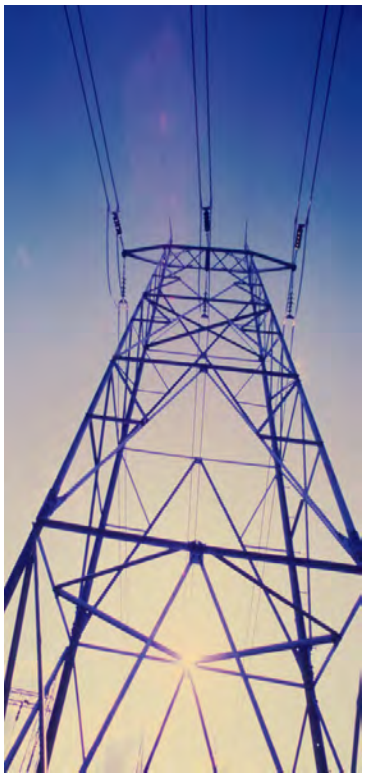
The Government will also take steps to enhance cyber security practices within government agencies.

Key initiatives:

- Establish a National Cyber Security Centre within the Government Communications Security Bureau.
- Implement steps to improve cyber security practices in government agencies.

Priority 3 – Incident Response and Planning

In light of the global growth in significant cyber security incidents, emergency preparedness is increasingly important. The Government will revise its cyber incident response plan to ensure New Zealand is prepared to respond to the evolving and increasing cyber threats.



Through the establishment of a National Cyber Security Centre, the Government will build on New Zealand's existing cyber security capability to plan for and respond to cyber incidents. The National Cyber Security Centre will absorb the current functions of the Centre for Critical Infrastructure Protection (CCIP).

The preparedness of New Zealand businesses to respond to cyber attacks is critical to New Zealand's cyber resilience. As new and more sophisticated malware and attack tools are developed, it is increasingly important for businesses to have measures in place to identify, assess and respond to incidents and threats.

The Government will work with critical national infrastructure providers and other businesses to support them to further develop their cyber security responses. This will include assessing the need for a New Zealand Computer Emergency Response Team (CERT).

Key initiatives:

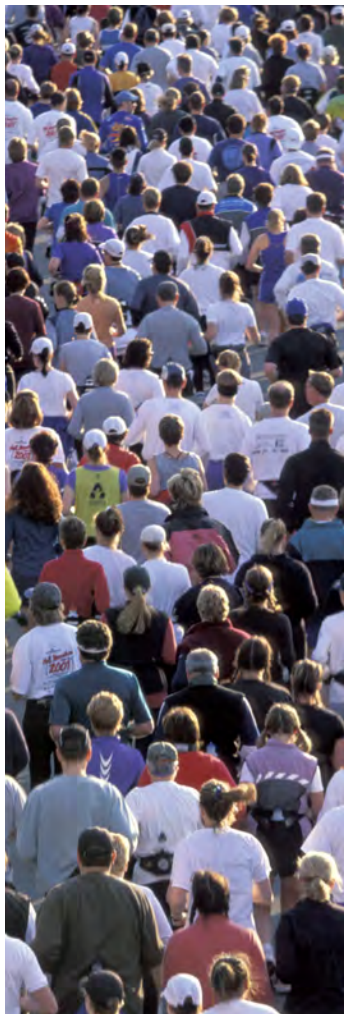
- Establish a National Cyber Security Centre, which will absorb the functions of the CCIP.
- Revise the Government's national cyber incident response plan.
- Expand work with industry, including critical national infrastructure providers and businesses to support them to review their cyber security responses.

Longer-term initiatives:

- Work with interested parties to determine the need for a New Zealand CERT.

Other Initiatives

Research and development is a key component in improving New Zealand's response to cyber security threats. Increasingly, organisations are seeking to hire the services of people with specialist cyber security skills and knowledge.



The Government will work with industry, universities and other educational and training institutions to determine appropriate solutions for meeting the demand for cyber security qualifications, training and research and development.

The Government will also work with industry, academia, government agencies and other relevant organisations to explore further opportunities to enhance New Zealand's cyber security response.

Maintaining an appropriate legal environment and ensuring international cooperation on cyber crime is important. The Government is working with international partners to improve co-operation on cyber crime. As part of an all-of-government response to organised crime, the Government is considering New Zealand's alignment to the standards set out in the Council of Europe Convention on Cybercrime.

Longer-term initiatives:

- Work with educational and training institutions to determine an appropriate solution to meet the need for cyber security professionals in New Zealand.
- Work with international partners on initiatives to combat cyber crime and determine New Zealand's alignment with the Council of Europe Convention on Cybercrime.

Government and Partnering Organisations

Ministry of Economic Development – the lead agency responsible for cyber security policy in New Zealand and implementing this Strategy.

www.med.govt.nz

Department of Internal Affairs – coordinates cross-government ICT initiatives and has units dedicated to addressing cyber issues such as spam and identity fraud.

www.dia.govt.nz

Government Communications Security Bureau – assists government agencies to protect their electronic information resources and communications systems.

www.gcsb.govt.nz

Centre for Critical Infrastructure Protection – supports critical national infrastructure providers to improve protection against cyber threats.

www.ccip.govt.nz

NetSafe – provides cyber safety advice to individuals, families, schools and businesses to promote safety online.

www.netsafe.org.nz

New Zealand Police – investigates and provides advice on electronic crime and computer related offending.

www.police.govt.nz

Ministry of Consumer Affairs – provides information and advice on how consumers can protect themselves and report scams.

www.consumeraffairs.govt.nz

Ministry of Education – supports *NetSafe* to provide cyber safety programmes for use in schools.

www.minedu.govt.nz

Ministry of Foreign Affairs and Trade – New Zealand's voice overseas contributing to the security and well-being of all New Zealanders.

www.mfat.govt.nz

The ORB – a simple and secure way to report online incidents which may break New Zealand law or breach legislation.

www.theorb.org.nz

New Zealand Security Intelligence Service – provides advice to Government about matters relating to domestic security.

www.security.govt.nz

Glossary of Terms

Botnet

A network of compromised computers running malicious programmes under a command and control infrastructure.

Computer Emergency Response Team (CERT)

Typically an operational team or centre that provides advice and mitigations against cyber attacks for businesses, government and individuals.

Critical national infrastructure

A term used by governments to describe assets that are essential for the functioning of a society and economy (e.g. electricity generation, gas production, telecommunications, water supply etc.).

Cyber attack

An attempt to undermine or compromise the function of a computer-based system, access information, or attempt to track the online movements of individuals without their permission.

Cyber crime (or computer crime)

Any crime where information and communications technology is:

1. used as a tool in the commission of an offence
2. the target of an offence
3. a storage device in the commission of an offence.

In New Zealand some of the most common examples of cyber crime include fraud, identity theft and organised crime.

Cyber security

The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.

Cyber space

The global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.

Hacking

An attempt by an unauthorised person, whether successful or not, to access an information system, usually for malicious purposes.

Identity Fraud

Any offence involving the misuse of a personal identity. The majority of identity crime is committed with the help of computers.

Intellectual Property

Includes a diverse range of commercially valuable assets including patents for new inventions, trade marks for marketing goods and services and copyright works like photographs, prototype drawings, literature and music. In business terms, intellectual property means that proprietary knowledge – a key component of business success – is protected.

Internet Service Provider (ISP)

An organisation that provides access to the Internet, commonly using copper, wireless or fibre connections.

Malware

Malicious software or potentially unwanted software installed without informed user consent, generally covering a range of software programmes designed to attack, or prevent the intended use of information and communications networks.

Phishing

A form of Internet fraud that aims to steal valuable information such as credit card details, user IDs and passwords by tricking the user into giving the attacker the confidential information.

Scams

Deceptive, uninvited contacts or promises designed to trick people into giving away their money or your personal information.

Social engineering

The practice of obtaining otherwise secure information by tricking, exploiting human traits of trust and helpfulness, or manipulation of legitimate users.

Spam

The use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately. The most widely recognised form of spam is email spam.

Trojan

A computer program that disguises itself as a useful software application, whereas its true purpose is to carry out and run a hidden, harmful transmission of material across a network.

Virus

A self-replicating program that spreads to other users by inserting copies of itself into other executable code or documents.

Glossary Sources:

Centre for Critical Infrastructure Protection.

Intellectual Property Office of New Zealand.

New Zealand Police Electronic Crime Strategy to 2010.

Microsoft Security Intelligence Report – January to June 2009.

Ministry of Consumer Affairs – 2010.