GCSB Director, Ian Fletcher, Speech to Rotary Club of Auckland

Stamford Plaza Hotel

April 14, 2014

Intro remarks

Good afternoon, thank you for the invitation to address you this afternoon.
I am very happy to be here and to engage with such a diverse group.
It is not often in this role that I get to talk in such an open forum and I am truly pleased to have the opportunity to talk to you about

- the work of GCSB
- To discuss some of the broader issues around the information security and why it is important to us all – small to medium size businesses, corporates, and other enterprise , not just Government agencies,
- and,finally I will touch on the balance of arguments around our desire for both privacy and security.

It is not that long ago that the name and work of the GCSB was largely unknown in New Zealand outside of the intelligence community.
Things are quite different now, and I do not propose to go into the details or background of that.
There has been plenty of commentary – much of it focussed on a very narrow aspect of our work.
However, I hope that when I have finished to day you will have a better appreciation of one of the more critical but often overlooked areas of our activity – cyber security.
Or, put simply our efforts work with Government, and Network Operators, and key New Zealand organisations to help protect our critical infrastructure and valuable intellectual property from a wide range of cyber threats.

Before getting into the some of the philosophical questions around privacy v security it is important to tell a little of the story around the changes underway at GCSB.

Our Change Programme

There is a lot happening within GCSB at the moment – some of it is in response to historical events and much more of it is founded in a real commitment to ensuring delivering our intelligence and information assurance functions in a way which all our stakeholders can have real confidence in.

We have committed to a Mission - protecting and enhancing New Zealand's security and wellbeing.

And we that in a way which reflects our Values – respect, integrity, commitment and courage.

The development and articulation of this Mission and Values is just one small part of our change programme.

We are well advanced in implementing the changes set out in GCSB Compliance Review undertaken by former Cabinet Secretary, Rebecca Kitteridge's and aim to have these substantially complete by mid this (2014) year.

Our wider change programme changes reflect a desire to take a more customer centric approach to our cyber security and intelligence work.

It also drives implementation of new operating and compliance models to support the new way we must function under recent law changes both the GCSB Amendment Act, and the TICSA legislation.

It also includes drafting new warrants and authorisations, new operational policies and guidance, and training staff. It also includes support for the new Commissioner for Security Warrants and new Inspector General of Intelligence and Security who provide oversight.

There is a lot happening

New Legislation

There can be no questions that the challenges and commentary around the issues which surfaced in late 2012 have impacted awareness and perception of our organisation.

They have also contributed to important legislation changes which now provide a very sound basis for our decision making going forward.

GCSB Act Amendments

The amended GCSB Act provides greater clarity around our ability to enhance the cyber security of New Zealand information, and information networks. It also defines more clearly the requirements around supporting the information gathering of other New Zealand Agencies.

The new legislation strengthens the oversight of our activities by

- requiring GCSB to maintain a written record of all warrants and authorisations in a form that is readily available for inspection by the Responsible Minister for GCSB and the IGIS. This supports a strong internal compliance culture which is overseen day to day by the management team
- increasing the IGIS's resourcing and reporting requirements
- ensuring warrants and authorisations are issued jointly with the Commissioner of Security Warrants where New Zealanders are involved, including for information assurance activities
- requiring us to report publicly how many warrants and authorisations have been issued
- committing to a robust review of the intelligence agencies in 2015 and every five to seven years thereafter.
- requiring greater transparency, through open public hearings for the financial reviews of the intelligence agencies.

These changes will enable us to work more effectively with key New Zealand organisations, providing advice on cyber security risk and known threats, and supporting their cyber assurance activities.

The legislation and policy governing our work in this area provides multiple levels of oversight.

Any support which requires us to look at data will require an interception warrant, authorised by the Minister Responsible and the Commissioner of Security Warrants.
Our support to any organisations will be covered by a Memorandum of Understanding, which, among other things will set out strict conditions around who can access information and limit the uses that information can be put to.
The information will only be able to available for GCSB's cyber security function, and all access will be logged and available for auditing by GCSB's compliance Unit and the Inspector General of Intelligence.

The TICS Act (TICSA)

The Telecommunications Interception Capability Security Act, which passed in early November last year (3013) sets out the basis for our work with Telecommunications Network Operators.
The Act, which comes into effect next month (May 2014) has two key functions – to modernise and "future proof" the lawful interception framework and to establish a new framework to guide how GCSB works with network operators to help ensure the security of New Zealand networks and information.
Importantly, the Act does not change the authority of agencies to intercept telecommunications, it does not change the existing privacy protections, and it does not require data to be stored, or require stored data to be disclosed. It only relates to real time interception.
The establishment of a network security section in the Act creates a framework which enables us to engage on a "good faith" basis with network operators to ensure the national security concerns can be factored into the design, build and operation of their networks.
This has been an area of significant focus for our TICSA team as we interact with Network Operators to develop and explain the policy and processes we will use to guide our interactions with them.
Just this morning I addressed one of three meetings we are having with operators over the next few days to go over the final draft of our guidance.
Guidance which was developed following a significant consultation process with them – something I think some in the industry did not expect, and something which they have indicated was greatly appreciated.

This closer engagement with industry and key organisations is something which there will be more of in the future as we increasingly work together to protect networks, critical infrastructure and important information.

This is just one small element of our mission – I think it is useful for you to have an overview of our work to give a wider context to the discussion.

What we do - GCSB functions

GCSB's core functions contribute to the protection of New Zealand's security and interests.

The Bureau plays a key role in enhancing New Zealand's cyber security.

The National Cyber Security Centre is part of the Bureau and through it we provided limited, specialist, support to assist key New Zealand organisations (government, state sector, critical infrastructure providers and key economic contributors), helping protect important information and ICT networks and infrastructure from advanced cyber threats.

Our focus here is high level – advanced, persistent threats, of the type generally undertaken by foreign states or state sponsored entities.

Our foreign intelligence function contributes to informed government decision-making through generating intelligence about the capabilities, intentions and activities of foreign organisations and foreign persons.

The Bureau also provides support, under warrant and in limited, special circumstances, to New Zealand Defence Force, the New Zealand Security Intelligence Service, and the New Zealand Police.

Changes to the GCSB Act provide a strong legal framework for this activity, setting out a clear requirement for access warrants and oversight for all activities.

NCSC Role

Information assurance and Cyber security

We see our cyber security mission as focussing on cyber threats which are generally described as "advanced persistent threats".

Advanced persistent threats are the sort of well researched software that will defeat or bypass the commercial security systems that most organisations use. These threats are characterized by motivation, funding and skill. They are sophisticated in their delivery, their ability to hide, and to remove and transmit valuable government or commercial data.

Within New Zealand GCSB is uniquely placed to be able to detect and guide response to this level of threat and intrusion.

Our cyber security response and support for other organisations is led by the National Cyber Security Centre.

The National Cyber Security Centre

The National Cyber Security Centre is a unit within the GCSB

As a foundation for policy, guidance and consultation work, NCSC staff undertake research around new technologies, emerging threats and pragmatic controls and solutions.

Much of this work leads into the production of published guidance such as the New Zealand Information Security Manual. (NZISM)

The NZISM provides policy, baseline standards and guidance around security of government information and information systems. The manual was last published in 2011 and is currently being revised to include updated information around topics such as use of cloud storage, mobile devices, BYOD and supply chain security.

The NCSC provides a range of services to help increase the resilience of New Zealand information networks, including publication of advisories on threat activity based on reports from NZ organisations and overseas.

The Centre also acts as a point of coordination for response to significant cyber incidents impacting New Zealand organisations.

It coordinates the exchange of information security across a range of sectors. These SIEs provide an e environment where organisations with common industry interests and threat exposure can share cyber risk information and response, in a forum which does not compromise any competitive relationship.

Government Information Assurance

GCSB, particularly NCSC staff are working with the Department of Internal Affairs, Government Chief Information Officer to support the establishment of a Government Information Assurance function within the GCIO office.

The NCSC will support this office with the provision of specialist technical input, threat advice and security policy input.

GCSB is providing input into the GCIO's establishment of an ICT Security Services Panel which will enable Government agencies to access a range of specialist security service suppliers.

The initial services offered through the panel will include risk management and assessment; security governance, architecture and design; security consulting and review; certification and assurance; source code and application review; network and application security testing; and computer forensics, investigation and security incident response.

We are also working closely with the GCIO and other Government security agencies to develop and update wider security policy and guidance.

This security guidance, covering physical as well as information security will be published as an unclassified document.

We also work closely with the National Cyber Policy Office – a unit of the Department of Prime Minister and Cabinet to contribute to policy and wider education initiatives – such as Cyber Security Awareness Week.. You can expect to see more of this in the near future. Watch out for a significant campaign, mid-year,

aimed a lifting the overall cyber security awareness and practice of both consumers and small to medium enterprises.

The threat

Why do we need to do all these things?

Quite simply because there is a significant threat out there which can have a real impact on our security and economy.

It is a threat which can result in disruption of critical infrastructure, result in large scale theft of personal information, removal of valuable intellectual property and impact on national economies and the machinery of Government.

The threat comes in a range of forms and from a range or sources. From cyber bullying, spam and fraud and one end, through to online sexual exploitation of children, commercial disruption of services and theft of intellectual property through to full scale cyber espionage and even, possibly cyber offensive.

Cyber Security - Threat Overview

GCSB's particular focus when we think about cyber intrusions is on so -called "advanced persistent threats". Other threats are typically criminally motivated, or politically motivated by particular issues.

Advanced persistent threats are the sort of well researched software that will defeat or bypass the commercial security systems that most organisations use. These threats are characterized by motivation, funding and skill.

There is real sophistication in their delivery, their ability to hide, and of course the long -term damage they can do sending valuable government or commercial data off to people who should not have it.

Where do these threats come from?

Cyber threats generally can come from a wide range of sources from state sponsored, but also from issues motivated groups or individuals, certainly from

criminal groups [who can be especially inventive and costly]. There can also be insider threats.

The International Threat Landscape

There are many high profile cyber incidents which have been reported in the global media.

Examples include last year's attack on Adobe Systems where the encrypted credit card details of 2.9 million customers were stolen. In addition, source code for a number of Adobe programmes was accessed – which in turn could lead to even worse hacking. Reports suggest that the personal credit card details of more than 38 million customers could have been accessed in this attack.

The month before that, Vodafone in Germany reported a cyber breach which had compromised the mobile phone records, including credit details, of 2 million customers.

And in December the details of 70 million credit cards were stolen in an attack on US retailer Target.

What is not so widely reported are the cyber espionage attacks on banking systems, and critical infrastructure and the theft of intellectual property by state sponsored actors and others trying to leverage their competitive advantage.

These two attacks are at the extreme end of the spectrum – but unfortunately they are becoming more frequent – and New Zealand is not immune.

The NZ situation

In New Zealand, as elsewhere it is very difficult to get an accurate picture of actual levels of cyber crime and cyber espionage.

While we have experienced an increase in reporting and recording of cyber incidents by the National Cyber Security Centre we believe there is a reluctance to report and that the true extent of threats and incidents on New Zealand networks is likely to be under reported.

NCSC statistics

The NCSC has seen a significant increase in the number of recorded incidents involving New Zealand government agencies, critical national infrastructure, and private sector organisations over the past few years.

When the centre first started recording incidents in 2011 there were 90 reports, in 2012 there were 134. We will be releasing the 2013 figures shortly and they will so a continuation of the trend for increased reporting of events.

This increase can be attributed in part to greater awareness of the importance of reporting incidents among New Zealand government agencies and critical infrastructure providers, and also awareness of the role and functions of the NCSC."

The New Zealand experience is broadly in line with international trends for cyber incidents. The majority of reported incidents – more than 60 percent- were targeted towards the private sector.

The nature of these incidents is highly variable from suspected denial of service attacks, and attempts of gain access to personal information such as passwords and banking details, through to full scale cyber espionage. However, it is important to recognise that the bulk of these recorded incidents are the result of self-detection and reporting.

Norton report

In other reporting on New Zealand, the 2013 Norton Symantec Report showed New Zealand is just as seriously affected by cybercrime, if not more so, than other countries.

It revealed that 69% of New Zealanders had experienced cybercrime, including 46% in the last year. The total cost of this crime was estimated to be $157 million.

Globally the estimated costs of cyber crime are staggering. While it is very difficult to get accurate estimates a collaboration between the United States based Center for Strategic and International Studies (CSIS) computer protection software giant, McAffee has estimated the cost of cyber crime in the United States alone as $100

billion annually and suggested that globally the losses could be upwards of $500 billion. Others have suggested the costs could be far higher.

So what do these threats look like?

Cyber Case Studies – (these have previously been used in forums such as the BHC event and will be in the publically the stats release

While our ability to provide "case studies" is limited by confidentiality, the following incident summaries give some idea of the range and consequence of recent incidents reported to us.

Spear Phishing Compromise

A number of New Zealand organisations reported receiving spear phishing emails. Spear phishing emails are targeted emails which try to pass themselves off as legitimate emails with attachments containing malware, and are designed to trick the recipients into opening them. Upon doing so, malware is automatically installed on the user's computer and can then be used by an attacker for further compromises.
In one case, a targeted spear phishing email containing a malicious .pdf file was sent to a number of email addresses for an organisation. Several recipients opened the attachment which then exploited a known vulnerability to install malware on the user's accounts.
Once the malware was installed, the perpetrators were able to access the network and get greater privileges to increase their access across the network. Ultimately they were able to collect and then extract sensitive information from the organisation

Spoofed Email Address

Private sector organisations reported receiving emails from scammers pretending to be employees. These "spoofed emails" were set up by scammers who were able to identify employees from the organisations' open source information.
The attackers used these names, or similar variations, to establish free email accounts. These web-based email addresses were then used to send emails to colleagues of the legitimate employees, requesting funds be paid on behalf of the organisation to bank accounts operated by the scammers. The organisation suffered financial loss as a consequence.

Ransomware Attack on company

A number of “ransomware” reports were received in 2013. In one case a small business reported they had received emails from outside of New Zealand threatening to disable their business unless funds were paid.

When no funds were paid the email senders – we call them threat actors – compromised the business’s servers, installed malware which encrypted their files, causing the owners to lose access to their systems.

Eventually the organisation was able to restore its network using historic back-ups, however they lost many recent records and were unable to conduct business for several days resulting in subsequent financial losses.

So - what can we do about it?

As you can see these are things which can have a serious impact on your business. We need to raise risk awareness in company boards and senior management teams, in the management of academic institutions, and across he community more generally.

That is where occasions like this are an important opportunity.

Aware, engaged management teams will influence organizational behaviour, set the right example, and determine the behavioural expectations for the organizations they are responsible for.

That means a real call to action. It means working up and down the supply chains which keep our economy going so that we do not just outsource risk and hope to avoid the consequences.

This is important. We know from analysis of successful cyber intrusions that advanced persistent threats are usually launched intelligently and perceptively against the weakest points in a supply chain or in an organization.

If your systems are strong, but the business which provides you with legal advice, your public relations service, or your accounting support is weak then you are vulnerable.

The organisations behind advanced persistent threats don't play fair. You don't need me to tell you that business is like international relations: if you're small, you still have to fight the big guys.

We also need an intelligent approach to protecting and managing our information. Aggregated information needs to be managed as an asset, with the same attention to systems, processes and behaviour you would expect to see in a well-managed manufacturing environment.

In the digital world, safety and productivity are as closely linked as they are in the physical world.

After all, if someone steals an asset from you and you haven't done all you could to protect it, that
suggests that you didn't value that asset as much as the person who stole it.

There is good evidence that companies which manage their intellectual property and their data well are significantly more profitable, competitive and resilient than those who do not.

I do not want you to think that I have come from the government to give you good advice which will simply cost you money.

Effective management of intellectual property is hard. It requires thoughtful, professional, painstaking work. But it pays off.

Good cyber security, allied with strong data and IP management is good for the bottom line. Indeed, in many knowledge based businesses, it is the bottom line.

While Government agencies such as GCSB, the DIA and NCPO can play an important role in understanding the threat-scape, and helping to create a more secure environment and more resilient networks, between 80 and 85 per cent of the

risk can be mitigated through implementation of sensible, and proven cyber security practice at organisation level.

Cyber is a risk that has to be “owned” Executive level. The challenge is far more wide-reaching than information systems security and MUST be addressed at a strategic, organisational level. Without this level of recognition and support, the ability of organisations to counter cyber-threats and attacks is severely compromised.

It’s a matter of thinking through the impact of cyber risks on:

- Governance responsibilities
- Audit risks and the whole assurance role
- Insurance risks
- Potential impact on future markets.

While the Executives and Boards cannot necessarily be expected to understand the full detail of the technical issues, they MUST, nevertheless, get to grips with the scope, scale and consequences of cyber-risks. Technologies such as cloud, virtualisation, social media and next-generation mobile computing are fundamentally changing how organisations operate in a cyber-world.

There are four basis steps that as Executives or mangers with responsibility for technology in your organisation you should ensure are in place.

- White listing - that means only running the software on your network and devices that your organisation has
  approved
- Keeping your systems patched.
- Keeping applications patched.
- Minimizing the number of users with administrator privileges.

As you can see, these are more organisational or behavioural steps, than technical They are all steps which each of us needs to take in our respective company or organisation.

And, the real benefit occurs when the whole supply chain for your company is protected. If you are outsourcing, ask hard questions of your provider:

- *Who are they?*
- *Where are they?*
- *How will they protect your information?*
- *What will they do if something goes wrong?*
- *Show me the proof.*

Security v Privacy

As I indicated at the beginning – I wanted to conclude with looking at an aspect of the security debate which has been largely overlooked in most popular commentary.
That is the balance which needs to be considered between our requirement - and desire - for security and the equally relevant and strong requirement and desire for privacy.
There are three debates which need to be considered:-

First, privacy. Although much of the media coverage of GCSB and other similar intelligence organisations focused on intelligence questions in the narrow sense, there is of course the wider debate going on about privacy and the role of what is called "big data". This isn't just about government data, but also privately held and commercially exploited data. The internet has the capacity to move relative power from producers to consumers by flattening asymmetries of information, giving people more informed choice. It also has the opportunity to create new centres of economic power through the creation of asymmetric information where big data is held for commercial purposes, especially where it is exploited or sold. Whether and how, and by whom, that process should be regulated is an important question for us all, which goes far beyond the narrow scope of the work of organisations like the GCSB.

Secondly, the internet is almost definitionally global. It brings together information and connection which is both "domestic" and "foreign" and converges and may even eliminate some of those differences. How should the internet be governed, and behavior on it regulated? This is not a trivial question: in the "real" world we see at a philosophical level a role for the state through the Hobbesian bargain, where we each

give up our private right to use force to defend ourselves to the state in return for the state establishing and enforcing general rules for everyone's benefit. We don't yet have a clear sense of who or how a similar framework should operate on the internet, and it seems to me to be important that we consider this carefully, not least because of the importance of taking account of the global nature of the internet and the connections that it creates.

Finally, there are important questions around security. This doesn't just relate to the security of the state or the protection in advancement of its interests. Rather, it relates to the intersection issues of privacy as described above, security (in the sense of the framework of rules) and identity. Most of us want to be able to use the internet for things like banking in such a way that our identity is authentically established and we are able to conduct our business in private as ourselves. The philosophy of identity on the internet seems to me to be an important question which we have yet to thoroughly explore.

Thank you, again, for the opportunity to talk to you today and to hopefully expand your understanding and awareness of the GCSB, our role and some of the challenges we face in our mission - *protecting and enhancing New Zealand's security and wellbeing*

Cyber reporting questions you might get asked

What should we do if we think there has been an attack or intrusion?

Any incident should be reported to us using our reporting line (04) 4987654. While we do not provide an indent response service, your reporting helps us form a better understanding of the threats faced by New Zealand

Who do we call at GCSB?

The National Cyber Security Centre has an incident reporting line. The number is (04) 4987654

So what is the threshold/nature of things we should come to you with?

We would like to be advised on any cyber security incident. Your reporting helps inform our understanding of the treats faced by New Zealand

What sort of issues should we be addressing ourselves?

GCSB's focus in on addressing advanced persistent threats to NZ Networks. These are the kind of threats which usually originate from foreign, usually "state sponsored" threat actors. They are frequently not able to be detected via commercial products. While you should report any incident to you us should work with your IT security staff and appropriately vetted external security providers for any initial investigation and advice on response.

What other options do we have to get assistance on cyber related issues?

The Department of Internal Affairs, through the office of the Government Chief Information Officer has worked with Government IT security specialists to identify and approve a panel of private sector security and related services providers. The providers, listed on the GCIO web site – ict.govt.nz (http://ict.govt.nz/common-capabilities/foundations/security-and-related-services-panel-/) – have demonstrated they can meet required standards and are able to be contacted directly to provide security support.