Speech given by the GCSB Director Ian Fletcher at the Gallagher Security conference held in Hamilton on 11 March 2013

Good morning

It's a real pleasure to be here this morning, to talk to you about GCSB.

Before I do that, though, I wanted to say how much I have been impressed by Gallagher, and the business it has become. We look forward to working with Gallagher and the rest of the New Zealand security sector in the future. The sector is thriving, and we already have the beginnings of a really strong partnership in place.

GCSB is the Government Communications Security Bureau. Some of you may know who we are and what we do, but others may not.

Firstly, we provide the New Zealand government and critical national infrastructure, that is banks, Telco's and utilities, with the technical support to ensure that its own systems and information is as secure as we can make it. And, as I shall explain, this work is rapidly expanding to include thinking about the security of information across the New Zealand economy, particularly in the face of the cyber threats and intrusions which have emerged as a real issue in New Zealand just as much as they have in other similar economies.

Secondly, we provide the New Zealand government with its foreign electronic intelligence service. New Zealand is a small country, and successive governments have found it really useful to have a foreign intelligence capability to help government make better decisions in foreign policy, and to be able to protect our Armed Forces when they are deployed overseas.

Thirdly, we are sometimes asked to assist law enforcement agencies because of the particular technical resources at our disposal.

Today, I would like to talk to you particularly about what we see in regard to one aspect of cyber threats and intrusions in New Zealand, and what we can do about them.

Before I do that, let me set out some of the concepts. Our 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 commercial security systems.

These threats are characterized by motivation, funding and skill. There is real sophistication in their means of 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.

I should say that I consider that data held on a company's computer systems is for all practical purposes a form of intellectual property. The effective management and husbanding of intellectual property is a whole topic by itself, but one which is very relevant here.

Where do these threats come from? Cyber threats generally can come from state actors, but also from issues motivated groups or individuals, certainly

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

What does the threat scape look like?

What you have been seeing in the news media around the world reflects what we see here in New Zealand. In other countries you will have seen the recent report released by Mandiant, the reports of the attack on the New York Times, the rather serious attack on the IT systems at Saudi Aramco, criminal attacks in Australia where systems were encrypted, and a ransom demanded for their decryption.

In New Zealand the National Cyber Security Centre 2012 incident summary reported an increase of nearly 50% in serious cyber intrusions reported to us, compared to 2011. Up from 90 to around 130. These are incidents that met the threshold of putting New Zealand government information or New Zealand's critical national infrastructure at risk, and we know from international experience that this is likely to be very much the tip of the iceberg.

This really matters. Digital technology has opened real economic opportunities for businesses in New Zealand, reducing the effects of our geographic isolation and small size. It's been encouraging and exciting to see how companies have been able to respond to this opportunity, and the result has been real economic diversification at home and real economic integration with our trading partners.

But with these opportunities come extra risks. Our challenge, both in government and in partnership with business, is to manage those risks so that we can continue to really take advantage of the opportunities. Easy to say, but quite hard to do.

The New Zealand government takes cyber security seriously, and we are seeing governments around the world putting extra resources into cyber

security. The New Zealand government works increasingly closely with business in New Zealand, and with our international security partners to ensure that their critical national infrastructure can continue to operate safely, and that criminal activity can be prevented, and if necessary detected and prosecuted.

The good news is that these are threats which can largely be managed in the corporate setting, as well as in government, provided we face up to the reality and to the significance of the challenge.

One thing is clear. Cyber security is a concern for the whole organization, be it a government organisation or a business organisation. It has traditionally been seen as a technical issue or matter for the folk down in IT rather than a matter of corporate risk. Yet the lessons are clear: if it goes wrong, it can amount to an existential threat. It's a matter for the CEO, not just a CIO.

What can we do about it? Firstly, we need to raise risk awareness in company boards and senior management teams, in the management of academic institutions, and in the community more generally. Aware, engaged management teams will influence organizational behaviour, set the right example, and determine the behavioural expectations for the organizations they manage.

We need a sense of urgency. Damaging cyber intrusions are taking place right now. 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 countries and groups that launch 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. To my mind, that raises serious questions about management values and even competence.

Interestingly, it's not that hard: our Australian counterparts have published research showing that they are just 4 steps that can reduce your risk by between 80 and 85%:

White listing: that means only running the software 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 organisational behavioural steps, not technical ones.

These are all steps which each of us needs to take in our respective company or government organization. But as I have already explained, 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. Your own system may be safe but is your lawyer's, accountants, payroll providers …

I think that the concept of herd immunity is relevant here: like vaccination, our economy and society will be more resilient in the face of these threats if most of us have taken the right steps, even if one or 2 have not.

These threats are not called viruses for nothing, and we need to apply the insights of epidemiology are relevant to information technology.

A final thought before I close.

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.

So what should you be doing? Let me leave you with 4 things to take away.

Firstly implement those top 4 steps if you haven't already done so, and report incidents so we can all learn from them. The kind of self reporting culture which has made aviation so safe is one we need to emulate.

Secondly work across the business community, with your suppliers and your customers to systematically think how to protect information and networks.

Thirdly work across the security sector and with government to think about the talent and skills we going to need now and in the future. As more businesses come to see that good cyber security generates profits, the demand for people with the right skills and commitment will grow even faster. We need to send the right signals to universities, schools and to young people themselves.

Finally give the government good feedback. Government has responsibilities to set the legislative framework, to take care of its own information, to create the kind of international security partnerships which will support the business community and to generally create the conditions for business success. The government needs to know how it is doing, where the gaps are and what needs to be done. This sort of feedback is management information for policymakers.

And that's really why I'm so pleased to be here to talk to you today: to continue to build the foundations for the strong partnership we are all going to need to deal with the threats of the cyber world effectively, so that we can really enjoy its benefits.

END