Speech Notes for New Zealand Information Security Forum
11 April 2013

Paul Ash, Manager
National Cyber Policy Office
Department of Prime Minister and Cabinet

CYBERSECURITY: WHY IT MATTERS FOR NEW ZEALAND

Good morning. It's a pleasure to be here this morning, talking with the NZISF. Thank you for this opportunity.

I've called this presentation **Cybersecurity: why it matters for New Zealand**. I expect that's a topic this audience already knows a lot about. Given that, I'm keen we have plenty of time for questions – to focus on what most interests you, and to ensure this is a two-way conversation. But first, some background.

Cyberspace – The Bright Side

Fundamentally, cyber security matters to New Zealand because connectivity matters to New Zealand.

The Internet has brought real, direct benefits - economic, social, cultural - to New Zealand. It continues to do so as technological change drives business and other changes. This really counts.

For New Zealand, enhanced connectivity is a crucial driver of economic growth. Connectivity has reduced the effects of our geographical isolation and it has helped to balance issues of scale – the size problem. It has opened real economic opportunities for New Zealand businesses.

It's been encouraging to see how New Zealand companies have responded strongly to the opportunities this has created. The phrase "weightless exports" now has real meaning. Commercial services exports are a key driver of growth – and one of our fastest growing export sectors. Companies such as Diligent, Xero, Orion and Open Cloud are obvious examples. There are many more – and more to come.

That growth is happening organically – entrepreneurs recognising opportunities and pursuing them. Government agencies are putting effort into improving the environment for this growth – from working directly with exporters through to delivering enabling policy settings.

One quick example. The recent recognition that New Zealand's Privacy Framework meets EU standards and is adequate for data transfers to occur might sound arcane, but it is a key enabler for trade and commerce. New Zealand is the first country in the western Asia-Pacific to achieve this – which opens new opportunities.

We'd expect to see this economic activity trending further upwards as New Zealand businesses realise the benefits of enhanced connectivity.

More broadly, New Zealanders in all walks of life are connecting to the Internet and realising opportunities. UFB and RBI rollout will see this trend increase. Internet use is becoming ubiquitous in homes, businesses and educational institutions. Researchers are collaborating with peers through initiatives such as the Karen Network and REANNZ. New Zealand's intellectual property is being developed on networks that connect our brightest minds with each other and the rest of the world.

In sum, the ubiquity of the internet is connecting New Zealanders to the rest of the world in ways that were once only the stuff of dreams.

Cyberspace – the Dark Side

With these opportunities come extra risks. Threat actors, whether cyber spies or cyber criminals, increasingly use cyber space to gain access to personal information, steal businesses' intellectual property, and gain knowledge of sensitive government information for financial or political gain or other malicious purposes.

New Zealand's traditional defences - time, distance, oceanic barriers – do not protect us from cyber threats. The cybersecurity threat to governments, businesses, critical infrastructure providers and individuals is real; threats can come from any person with a computer that has an internet connection in any part of the world. For threat actors, the Internet dramatically scales their operations.

For example, before the Internet the operations of organized crime cartels were largely bound to a particular location or geographical region. Only a few very large, very well-resourced cartels could operate across continents and oceans. Now, even small criminal outfits, provided they have the requisite technical skills and tools – and these can easily be hired or brought in cyber crime forums on the deep web – can readily target individuals, businesses, banks and governments on the other side of the world. New Zealand is not isolated from this threat.

What does this threat landscape look like? Put simply, cyber intrusions are becoming more advanced, more sophisticated, and more pervasive. And those behind them are coordinated, well-funded, and investing heavily in exploiting the digital environment.

Efforts are increasingly targeted at intellectual property and proprietary information held by business, as well as at government, critical infrastructure providers, and individuals. Countries like New Zealand face threats that broadly fall into three categories:

Criminally motivated threats - manifested through cybercrime, generally with the objective of profit (or harm) through criminal activity.

Politically motivated threats - generally driven by a particular issue or cause, these can cause significant damage and disruption to target systems and operations.

Cyber espionage; also known as advanced persistent threats - these are well-researched, well-resourced, and often capable of defeating commercial security. They reflect motivation, funding and skill – in their delivery mechanisms, ability to hide once access is gained, and in the damage they can cause.

Who's behind the threat?

The threats come from a range of sources – individuals or issues motivated groups, state actors, criminal groups and, in some instances, insiders.

Attribution is a major challenge. It can be extraordinarily difficult to understand the source of a threat. Often the more sophisticated threat actors will go to extraordinary lengths to mask the source of a threat.

What's the scale?

This is difficult to measure. Victims – whether individuals or commercial entities - are often reticent about coming forward. But we do know from our experience, and from that of others, that the problem is serious.

You will have seen reports from other jurisdictions of an extraordinary increase in reported intrusions. You will also have seen reports of the cost – direct financial losses, loss of future earnings through intellectual property theft, and the potential for damage to critical systems.

New Zealand is not special. These problems are affecting us. In 2012 the National Cyber Security Centre incident summary reported an increase of just on 50% in serious cyber intrusions when compared to 2011. By serious, we mean incidents that met a threshold of putting New Zealand government information or critical national infrastructure at risk. There were 134 of these incidents and we think this number is likely to be the tip of the iceberg. This year already there have been 76 reported attacks.

The National Cybercrime Centre at New Zealand Police is also dealing with a steady and large flow of reported cybercrime incidents. As a comparison, the UK's National Audit Office estimated cybercrime to be costing its economy between £18bn and £27bn a year. New Zealand is not special. Estimates for the cost of cybercrime in

New Zealand are hard to verify, but most are in the range of hundreds of millions of dollars. In 2010 it was estimated 70% of New Zealanders had been the targets of some form of cybercrime, with the most common complaints being computer scams, fraud and viruses/malware.

In the aggregate, this adds up to a significant national security risk. And for individuals and organisations cyber security events can be devastating.

What can we do about this?

The good news is that there are things we can do. That starts first with understanding why we manage risks - to enable New Zealanders to take advantage of the opportunities of the internet.

It also requires understanding that cyber security is a shared responsibility. Government, the private sector, critical infrastructure providers and individuals all have big roles to play in lifting cyber security standards.

Government recognises it plays a significant role. It has a responsibility to protect its own systems and to assist critical national infrastructure providers. It plays a role in helping to provide a safe digital environment for businesses and individuals. It has a responsibility to establish sound organisational, policy and legal frameworks. And it can help to make New Zealanders and businesses more aware of cyber threats, and how to take measures to protect themselves.

As far back as 2001, the Government established the Centre for Critical Infrastructure Protection to improve the security of New Zealand’s Critical National Infrastructure from cyber-based threats.

The cyber landscape and the threats we face have evolved dramatically since then. This has led to an evolution in New Zealand policy.

In June 2011, the first *New Zealand Cyber Security Strategy* was released. It set out three priorities for action:

- raise 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.

As part of the Strategy, in September 2011 the National Cyber Security Centre was established in the GCSB.

The Centre is a successor to the CCIP. It provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

For example, the Centre has just helped to facilitate the development of voluntary standards for a group of operators of Industrial Control Systems. These critical infrastructure organisations all operate industrial control systems, which allow centralised supervision and control of remote assets. The safe operation of these is fundamental to keeping New Zealand functioning well.

The group has worked successfully together with NCSC on developing voluntary security standards – drawing deeply on the experience and knowledge of the operators and the technical experience of NCSC staff.

As Mike Judge from Genesis Energy put it “this work has allowed us to safely discuss cyber security issues and work together with industry to develop best practice and share information.”

At the same time as the NCSC was set up, in late 2011, a Cyber Security Plan for Government was launched. The GCIO and GCSB play a significant role in this initiative and other efforts to lift information security in government.

More recently, in July 2012 the National Cyber Policy Office was established in the Department of Prime Minister and Cabinet, to lead and coordinate cyber security policy. The NCPO has a whole of government role, and is responsible, among other things, for implementation of the cyber security strategy.

Consistent with the Strategy, other units, working across multiple agencies, are tackling issues such as scams, spam, and identity theft and electronic crime. Agencies are working on New Zealand’s framework for dealing with the growing issue of international cybercrime. The Ministry of Justice has delivered recently-announced work, drawing on the Law Commission’s efforts, to address the problems created by cyber-bullying.

The Government is also actively working with partners in the international discussion on cyber security – a growing part of the agenda. It’s important for our international reputation that we constructively engage in this emerging discussion, and that we are demonstrably seen to be improving our own cyber security.

Just as many of the cyber security problems have an international dimension, so too many countries will look for international solutions. In regional bodies such as ASEAN, APEC, PIF and the ARF - all of which are now discussing cybersecuirty issues in one form or another - in bilateral work with partners such as that recently announced with Australia and the United Kingdom, or as cyber security issues emerge in multilateral bodies such as the UN or WTO, it is important New Zealand contributes.

That contribution is not just around discussion of norms or rules of the road, but also in providing assistance and collaborating with others. The NCSC, for example, works with others as part of the Asia-Pacific CERT network. New Zealand Police, supported by MFAT, have led ASEAN training on cybercrime. And MFAT has taken part in the initial work among Pacific Island Forum members on the challenge of addressing cybercrime.

There’s also a big role in all of this for those outside government – and we are seeing cyber security effort in a range of sectors. Universities and research institutions are doing work on cyber security. The private sector is leading the demand side of efforts to lift cyber security work force capability. Organisations such as Netsafe work on cyber security awareness – we sponsored the initial cyber security awareness week with them last year and will do so again. And entities such as Internet NZ, the NZITF, and this forum - the NZISF - play a key role in pulling together those who work in this space.

A Formative Process

What we are seeing here is the adaptation of existing security structures and practices to meet cyber threats, and indeed the emergence of new, and possibly quite radical, structures, practices, and ways of thinking about security.

At the moment this is a formative process, and we’re not there yet. It’s also quite exciting, as ideas are being generated, tested, and worked through. One of the things we’re excited about is the idea of cyber security as a collaborative endeavour.

Traditionally the state has been the primary provider of security from threats, whether foreign invaders, spies, or criminals. Cyber security is forcing us to revaluate that view, to consider the notion of cyber security as a collaborative, multi-faceted endeavour between government, the private sector and citizens.

This is partly because the infrastructure of the Internet and cyberspace, and the information flowing across this infrastructure, is privately owned and spans jurisdictions. And partly because cyber security threats cannot be neatly separated or quarantined from the way we use cyberspace in our enterprises and our lives.

If there is such a thing as a ‘front line’ of cyber security, then it exists not in some far-off theatre of war, but instead runs through our houses, schools, small and medium enterprises, large corporations and banks, and government agencies.

What this suggests is that everyone, not just the state, has a part to play in defending our society and economy from threats. The Government may take the lead in some areas, may galvanise or facilitate action in another area, and might take a supporting or enabling role in a third area.

Conclusion – how do we take this forward?

I’d like to conclude by acknowledging again that we don’t have all the answers here, and by asking you some questions to kick off discussion.

If we accept that cyber security is a collaborative endeavour involving all of us – government, private sector, citizens - working together to secure ourselves against threats, how can we take that forward?

What are some practical ideas that could provide real results without becoming talkfests or imposing undue costs?

Beyond the overview I’ve outlined, are there things we are doing that you’d like to know more about?