Address to Electricity Networks Association

23 June 2015: Cyber security and its relevance to the electricity distribution network/critical infrastructure

Thank you for inviting me here today to speak with you. It's great to be here and to discuss cyber security and its relevance to the electricity distribution network and other critical infrastructures

I am Una Jagose, the Acting Director of the Government Communications Security Bureau. I started in late February this year, coming from my role as Deputy Solicitor-General, Crown Legal Risk at the Crown Law Office. And, as you may have seen last week, that acting stint has been extended until the end of March 2016. I am really excited about having the extended period in this role: the GCSB is a great place to be working; a lot has changed in the last few years and there is more change coming. The year ahead holds a lot of promise.

One of our significant areas of focus will be on cyber defence and security. You probably know, given the invitation to the Government Communications Security Bureau to speak to you today, how important cyber security is: Government and private organisations as well as individuals are being attacked daily. We have seen plenty of well publicised examples of this recently; both here in NZ and overseas.

Briefly, to ensure common understanding, the GCSB has three statutory functions:

- Gathering and analysing foreign intelligence
- Helping other agencies (Defence, Police and Service), and (today's focus)
- Information Assurance and Cyber Security

The Information Assurance and Cyber Security functions are delivered by the National Cyber Security Centre (NCSC) that sits in GCSB, established in 2011. Its part of the GCSB .

Its function is to provide "*enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.*"

Countering these threats is a shared responsibility, and the government works in partnership with industry, non-government entities and academia to improve New Zealand's cyber security. The role of the NCSC is to protect government systems and information, to plan for and respond to cyber incidents, and to work with providers of critical national infrastructure to improve the protection and computer security of such infrastructure against cyber-borne threats.

And we have some regulatory responsibility under the Telecommunications Infrastructure Communications Security (TICSA) Act.

Focusing on cyber security, our key roles are to:

- Provide support and advice to help develop secure networks with a focus on National Critical Infrastructure (potential harm to NZ security and economic wellbeing)
- Detect and respond to sophisticated cyber threats
- Coordinate and assist responding to major cyber events

The NCSC role is broadly split into two parts:

- Outreach and engagement functions
- Incident Management and Response Team

Cyber Security Operations include:

- Threat discovery
- Investigations where threats have been identified
- Threat reporting to customers and to partner organisations
- Forensic analysis

However, cyber security is not just a technical issue. Information in organisations is under threat from a number of overlapping areas.

My aim today is to encourage you to see information security through a lens of people, places and systems:

- The people risk – an insider threat can be as damaging as a cyber attack. And your people can also be the cause of vulnerability – whether deliberately or by failing to follow security protocols.
- The places risk – premises need to be secure to prevent physical access. What are your boundaries – in cyber terms you have to think of them as more than the physical reaches of your organisation. What is the reach of your information and data sets? That's the boundary. Now think again – are you sure your boundary is secure?
- Following that, the systems risk is probably obvious, and doubtless your IT teams assure you of security of those systems. But have you considered outsourced IT service providers:
    - what are their security arrangements?
    - Is their resilience regularly tested?

    - Contracting out won't prevent cyber attacks on your business.

Think of your information as a supply chain – from start to finish – its only as secure as the weakest link in that chain.

So you think your organisation is secure. What about:

- service providers?
- legal advisors?
- consultants and contractors?
- Device security?
- User habits?

    - if any element of your connectivity is insecure, you are vulnerable.
        - And, also ask, are you creating vulnerabilities for others?

Again, at the risk of the stating the obvious, cyber security is not just about your operational networks. It's about keeping your customers' information secure.

This really matters to the public, and they don't have a great deal of confidence – in you or in us! The Bureau sought some independent polling when we had been in the public eye a fair bit towards the end of last year (sample size 1000), and on the issue of who is better at keeping your private information secure … the government or private sector .. what would be your pick?

- 30% of people believe the Govt is better at keeping private information secure

- 24% believe the private sector is better at keeping private information secure

- 18% believe neither can manage this.

Somewhat mysteriously, folk in the provincial cities are the most sceptical … 27% believe neither the Government nor private sector are better at keeping private information secure. Together we have a lot of work to do here, both to build confidence that as connectivity grows and becomes, as it has, the norm, we are able to manage private information and security…

There are three common positions agencies take on cyber security that influence how an organisation prepares and responds to cyber threats. Each position is wrong, in my view, and risks a cyber stance that exposes, rather than reduces, the agency to vulnerabilities.

- Organisations don't believe they have anything of value or underestimate what information is of value. That position leads them to think they are not at threat. But your data is valuable. Your customers certainly think so. We live in a data economy and are not only seeing data being stolen, but combined with other data sets to create commoditised information with commercial value or changed along the way.

Data is monetised now more than ever before and the trends indicate this will increase.

- NZs geographical isolation has traditionally meant we are safer from some of the risks we see overseas – but of course connectivity to the internet knows no geographic boundaries, and, accordingly, there is vulnerability in connectivity.
- Taking a risk avoidance position. This is only successful if you can be sure to have better defence than every potential attack. That's not likely, I'm sorry to say. It is better to have a risk acceptance strategy: mitigate the risks and prepare your resilience to those risks being realised at some point.

For GCSB (and the NCSC) our focus is on technology. In broad terms, threat stems from the rapidly changing nature of the internet, which was not designed with security in mind. The scale and pace of growth is almost unimaginable, and means vulnerabilities are constantly being introduced, protected against, and re-formed – rediscovered and so on it goes. Connectivity to the internet is everywhere; crossing national and international boundaries, time zones, and allows previously disparate groups to connect.

A couple of years ago there were as many internet connected devices in the world as there were people. Current growth trends point to there being three times as many internet devices as there are people in the world by 2017. Nearly 2 billion people use the internet as their preferred means of communication.

It's a scale that offers massive opportunities, both for those who have good intentions, and those who do not.

On the not-so-good side, the trend is moving from just simply stealing data to manipulating or destroying it. For example the much publicised Sony hack where we saw more than the theft of a movie before public release but a cyber attack to seriously threaten the company and its infrastructure, at huge cost. And more recently the United States Office of Personnel Management (OPM) security clearance computer system database of personal information relating to military and intelligence officials was discovered as inhabited by hackers. More than 4m US government workers private details were taken. And the hack was not

discovered for more than a year, giving the adversary ample time to steal as much information as it wanted. And just this morning in the Dominion Post is the story of 1400 passengers stranded at a Warsaw airport as hackers took over the airline's systems.

We, and that includes you, need to plan accordingly – damage that is not detected is the most dangerous. From undetected intrusions we can expect corruption and misuse of personal information, research data, business data.

Jonathan Hoyle, former Director General of GCHQ - our counterpart organisation in the UK, has cautioned that what they are seeing is significant loss of Intellectual Property from UK organisations – and there is no reason why it's not happening here.

What the data tells us is that the threat is constantly evolving. Its multi-faceted and transnational.

- If your strategy relies on responding to threats as they emerge, I'm afraid it will fail as an effective strategy.

So, what's the answer? One significant part of it is that the basics matter in cyber security– but they are not as commonly implemented as you would think.

Most cyber-attacks succeed because basics aren't followed. Even though there are some adversaries who have access to the most sophisticated cyber attack capabilities, they will always try the basics first. Afterall, what burglar doesn't try for an unlocked window first, even if she can hack through your house hold security system? So too, an adversary will not risk deploying their expensive, covert and hard won cyber-attack capabilities if they can slip in the 'open window' in your system.

So what are the basics? At a high level ...

- Implement commercial grade IT security

- Have clear privacy and security policies that are known, audited and checked

- Do your thinking about security and the way that you deal with customers, consumers and information *before* an incident

- Know what information you have and what information you value

Our Australian counterpart, ASD, has published mitigation strategies and the top 4 go a long way to addressing issues. They are simple:

- Patching systems.
- Patching applications.
- White listing - ensuring that only authorised software can be run on your systems (not stuff from home or malicious code sent over emails).
- Limiting the privileges of network administrators and controlling passwords.

This is all basic best practice, not done well across the board, but very important to get right.

The GCSB strategy to deal with cyber threats has multiple layers and is more complicated, (but it has a certain logic). Its a layered strategy to deal with cyber threats:

- We provide high grade crypto services to protect critical data of national importance
- We conduct technical inspections and accredit networks processing critical data of national importance
- We maintain relationships with key public and private organisations of significance to the security and economic wellbeing of NZ. This includes the Security Information Exchange Groups that we facilitate and the CORTEX programme which I will share some insights from, shortly).
    - On SIEs, about 6(a) of the 6(a) companies here today are part of the control systems SIE which we co-chair. It's a valuable forum for the exchange of information and ideas. One of the very practical things done under this SIE – and a brilliant display of private and public sectors working in concert to achieve joint aims – is

the development of voluntary security standards for industrial control systems, providing a baseline of cyber security protections. (at www.ncsc.govt.nz)

- We are keen to hear about how we can work more closely with you in assisting in the cyber security area.

- We provide well-researched information assurance guidelines following international standards and best practice
- We have developed an excellent understanding of threats facing NZ
- We provide cyber security and incident response services to deal with threats to national critical infrastructure
- And we promote the move to a mature security culture through outreach and engagement

I'd like to encourage you to check that your organisations are aware of the NZ Information Security Manual. It has been around for a while in various forms. The latest iteration has become a living document published under the Protective Security Requirements mandate, but is constantly updated as key information comes to hand . It includes threat research from classified and unclassified information sources. Its on the NCSC website – GCSB.govt.nz will get you there, or ncsc.govt.nz.

Much of the cyber security thinking has been done for others and advice encapsulated in the ISM. You don't need to understand the threat itself in detail. Just implement the advice and understand the residual risk to your organisation – take a risk based approach.

[note the IoD cyber risk practice guide released yesterday and its key messages]

We also work closely with other organisations on the cyber threat. We're well connected with:

Police – National Cyber Crime Centre (NC3)

DIA on privacy and IA

Connect Smart (NCPO) – an awareness raising initiative that is running this week. The NCSC encourages home and small to medium enterprise computer users to

participate in these Connect Smart events and activities, and to ensure they are adopting the best possible information security practices. Details of Connect Smart events and activities can be found at www.connectsmart.govt.nz

Netsafe

NZ Internet Taskforce (Largely volunteers in the commercial sector)

Together, we are trying to ensure that we work together to serve the best interests of all NZers, with our different focus/areas of interest.

The CORTEX programme I mentioned previously was announced publicly last year. Its about providing *enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.*

CORTEX is a cyber-defence programme, conducted under the GCSB Act. It was approved by the Government in the middle of last year and is being rolled out in phases. It is available to high value public and private organisations to protect against advanced malware. Some of the new capabilities have been deployed, and there has been a corresponding increase in GCSB activity. For example, in the first 10 weeks of 2015, we resolved more cyber security incidents than we did in all of 2014. We don't believe that's because of an increase in the volume of incidents so much as our improved capacity to identify and resolve incidents promptly – thus minimising the harm to important New Zealand organisations.

Some examples of what we have seen or been involved in recently, include:

- An Auckland firm's computer network attacked by an overseas-based criminal group
- Resolving a long-term compromise of a major IT firm
- A telecommunications provider being supported after seeing suspicious, overseas-sourced activity on their network

- Helping private sector organisations suffering ransomware and denial of service attacks.

Some incidents require our assistance, others can be resolved with some advice, and others again are managed by the entities themselves when they are aware. As I said earlier we make sure we use what we are learning in the CORTEX progamme more widely, through SIEs and other advisories – stripped of any classified content.

These examples are intended to show New Zealand government and private sector entities are in fact targets and victims of malicious actors. We cannot be complacent about it. But plenty is being done, with government, industry, academia and NGOs working together to understand better the threatscape and how to build our resilience to it.

Resources: on our website: issues for consideration at Board level. A simple 10 Qn checklist to get you on your way to understanding cyber security as part of the whole enterprise. And a more detailed publication for executives to lead discussions within their agencies, and with Boards, about cyber security. Its no longer a matter than can be relegated to IT responsibility.

So, my final thoughts

Understand the value of your information and data sets

Accept that you cannot avoid your cyber-borne risk

Instead, take the posture of managing risk and building resilience

Cyber hygiene basics - if done properly – manage a significant part of your risk

But remember: It's not just about technology … people and places are just as important as sources of vulnerability.