Good morning, thank you very much for the opportunity to talk with you today, it is great to be here. I am looking forward to sharing some insights into the work of the bureau, and our information assurance role in particular.

I plan to cover off some of the background to our role, and overview of why it is relevant for you and your work.

I welcome the opportunity to take questions at the end, and I will answer them as fully as possible, although of course there will be some questions I am not able to answer, or to answer as fully as you’d like, given the nature of what we do.

Part of the GCSB’s mission is to “*to ensure the protection, security, and integrity of communications, and information infrastructures of importance to the Government of New Zealand,”*

In short that means, help protect New Zealand’s important information and information systems –this very much includes the work you do and the information systems which you use to do it on.

The sense of comfort we feel tucked away at the bottom of the South Pacific away from many of the worlds troubles is less-and-less valid these days and especially so in cyber space.

The potential for having your research targeted by people who would steal the economic or social advantage it might provide is very real.

It is our job, and a function more broadly across Government ICT and the Information Security Sector to help you respond to this risk.

For us, the bulk of our support comes through the work of our Information Assurance and Cyber Security Directorate (IACD), which incorporates the National Cyber Security Centre.

The IACD does more than just in cyber security in the generally accepted sense of the term.

Some of the things you might not know about include;

* That we provide high grade cryptographic services to protect critical data of national importance
* We conduct technical inspections and accredit networks processing data of national importance
* We provide information assurance and security guidelines via the government Protective Security Requirements and the NZ Information Security Manual
* Our work includes the CORTEX initiative which I will talk in more detail on later.
* We also provide a point of national contact and coordination for reporting and sharing information on cyber threats and, in the case of some nationally significant information systems supporting response to those threats.

Where possible we work with security vendors to pass on threat information which can then be incorporated into more widely available, commercial products.

**The threat scape**

Like other areas of technology, the arena of cyber threat is very dynamic.

As technology pervades more aspects of our private and business lives the opportunities to exploit that technology for illegitimate means also grows.

The commercialisation of exploit kits (including in some cases 24/7 support!) means that even relatively sophisticated cyber threats can originate from threat actors with a fairly low skill base.

Reporting from well-known international security providers give some insight into the global scale of the threat. Symantec’s November 2015 update says they detected 19.4 million new pieces of malware (cyber threats) in November alone.

For the whole of 2014 they detected more than 317 million new pieces of malware – almost one million new threats per day.

And they say those threats are increasing in sophistication – making them more difficult to detect and analyse.

This means they are likely to operate undetected for longer and potentially cause greater harm.

In its 2015 “M-Trends” report, Mandiant noted that the median number of days that a threat was present on a network before it was detected was 205 (nearly 7 months). The longest presence they noted before detection was 2,982 days (more than 8 years).

This gives an adversary plenty of time to gain access and give themselves administrator privileges, conduct reconnaissance of the data in a network, package up what they want and send it to themselves, then disguise their tracks so it is difficult for the victim to identify what has been taken.

Mandiant reported that 69 percent of victims were notified of the compromise by an external entity, rather than having it picked up by their own internal systems.

At the Bureau we are also seeing continued growth in reporting of significant cyber incidents, although the reporting pattern is changing as more organisations – both Government and NGO - become involved in cyber threat reporting, response and education.

Of the 190 recorded incidents (slightly lower than previous year due to reporting changes), 114 were identified as targeting government systems, 56 targeting private sector, and a further 20 where the sector targeted was not identified in the reporting.

We believe that serious incidents are continuing to increase with a growth in threats at the more sophisticated end of the spectrum. In the latter part of 2015 the NCSC incident response team was recording an average of one serious incident a day.

The incidents we are seeing range in seriousness from the targeting of small businesses with “ransom ware” to serious and persistent attempts to compromise the information systems of significant New Zealand organisations.

Some of these threats come from well-resourced foreign sources. Sometimes they are targeting New Zealand organisations, others use New Zealand systems to target overseas networks.

Examples of the threats identified through our cyber security capabilities include;

* The targeting of officials from a key government agency through email and web site exploits to get personal information and potentially compromise the agency’s network. This attack was detected and mitigated before important information could be lost/compromised
* The use of a malware package, most likely purchased online, to target six significant New Zealand organisations. The threat was detected and mitigated through systems and support provided via our CORTEX capabilities.
* Identifying and tracing the source of a new cyber-attack method from a known major foreign threat source. The attack targeted several CORTEX customers. The “fingerprints” of this new threat were able to be passed on to our international partners, helping to reduce global vulnerability to this particular attack.
* Detecting large-scale targeting of a nationally significant organisation as part of a global campaign by known foreign threat source. The NCSC was able to work closely with the New Zealand organisation to contain the threat.

It would be easy to look at these examples and say *“well that is not us”*. I can assure this is not so, the scientific and research community is very much a target both here and overseas.

The confidential nature of our relationship (locally and internationally) means we cannot talk specifics in this forum, however we know of several instances in New Zealand where research organisations have been targeted by sustained spear-phishing campaigns in an effort to either harvest user information/ or to directly compromise systems. We know about some of this from self-reporting, while instances have come to our notice through other reporting.

On the international front there are many examples - one of the more serious we have been told about was a sustained, and repeated intrusions, into a major international research facility. The compromise existed undetected for several years and resulted in the exfiltration of gigabytes of data.

**CORTEX**

Part of our response to this growing risk, to help protect New Zealand’s most significant information and systems, is the CORTEX initiative.

CORTEX is an umbrella term for a mixture of passive and active detection and discovery, analysis and blocking tools, fuelled by a variety of inputs (signatures) including from classified sources.

The existence of the CORTEX initiative was disclosed by Government in September 2014.

CORTEX has only has one purpose: to counter cyber threats to organisations of national significance.

It is not about replicating existing information assurance capabilities – in fact we rely on all supported entities having a high standard of commercial protection - it is focused on countering foreign-sourced malware that is particularly advanced in terms of technical sophistication and/or persistence.

CORTEX customers include government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure.

There is a double gate (authorising mechanism) to CORTEX capabilities being provided to organisations.

* First, the organisation obtaining the capability must consent to receiving it – and agree to a number of conditions, and
* Second the capability must be authorised by the Minister, and the Commissioner of Security Warrants, under the GCSB Act

Information which we obtain can only be used for information assurance and cyber security purposes and the information can only be shared with the consent of the affected organisation.

CORTEX gives us an ability to detect threats to networks, and to tell protected organisations about those threats so that they can respond to them.

It enables us to provide targeted advice from our experts about the prevention and mitigation of cyber threats.

CORTEX usually involves deployment of a layered set of technical capabilities.

Initial detection occurs through automated means in the main– i.e. machines looking for indicators of malicious activity using information about previous successful or attempted cyber-attacks.

Rules limit the number of our people who can access the data and the Inspector General of Intelligence and Security is able to view a log of what occurred

Capacity constraints mean the CORTEX capabilities are only available to a limited range of organisations. However the benefits (threat information) are applied more widely through a range of approaches like direct interaction with customers, Security Information Exchanges, and the publication of advisories.

**SIEs**

Security Information Exchanges are dedicated to improving the protection and security of systems and networks from cyber based threats.

The SIE’s are designed to facilitate the exchange of information between its members, in a confidential and trusted environment, concerning threats, vulnerabilities and/ or incidents of electronic attack on a particular industry or sectors’ networks and environments.

There are two SIEs which help ensure the security of the work conducted by participants in this e-Research forum, the University Security Information Exchange (USIE) and the Crown Research Institute Security Information Exchange (CRISIE).

The University SIE has been going for a couple of years. The Crown Research Institute SIE was started in June last year (2015) and it has representatives from the 8 CRI’s. REANNZ is an associate member and is hosting this month’s SIE at the end of the conference.

Participation in the SIE’s is by invitation, agreed by the existing member organisations – this helps to ensure security issues can be discussed – even amongst organisations which are likely to be in competition with each other – in a high trust, confidential, environment.

SIEs provide a place for members to discuss;

* Cyber security strategies and policies that are appropriate for the Research sector,
* Recent cyber security incidents that have impacted on, or targeted their sector, and the strategies used to mitigate them
* IT security topics of interest that are unique to the Research sector e.g. how they walk the tightrope between keeping research systems safe, whilst allowing researchers the freedom to collaborate locally and internationally.

The goal is to share information and cyber incident experiences to raise the collective level of awareness and preparedness across the Research sector.

In closing, I wanted to leave you with some options for getting more information to help ensure your own personal information security and that of your work.

Of course, your first port of call should always be your own IT/Information Security shop. They are likely to be in touch with the latest trends, issues and advice and actively applying patches and protections to your systems. However if you want more information please check out the Resources section of the NCSC, ConnectSmart, and the NZ Institute of Directors – all of which have useful information for a range of different audiences.

And, of course, you can get in touch with us directly. You can email us through [info@ncsc.govt.nz](mailto:info@ncsc.govt.nz) or check out our websites [www.gcsb.govt.nz](http://www.gcsb.govt.nz) or [www.ncsc.govt.nz](http://www.ncsc.govt.nz)

Thank you very much for your time – I am very happy to take questions.