TRANSPOWER

Keeping the energy flowing

Waikoukou
22 Boulcott Street
PO Box 1021
Wellington 6140
New Zealand
P 64 4 495 7000
F 64 4 495 6968
www.transpower.co.nz

Cobus Nel
General Manager Information Services and Technology (IST)
DX mail code: SR56070. cobus.nel@transpower.co.nz +64 4 590 6956

2 August 2018

Paul Ash
paul.ash@dpmc.govt.nz
Director, National Cyber Policy Office (NCPO)
Department of the Prime Minister and Cabinet (DMPC)

Dear Paul

NCPO Cyber Security Strategy Submission

The cyber threat landscape is constantly evolving, and we practice risk management in a manner that reflects our responsibility as a critical lifeline utility in New Zealand.

We utilise Information and Communication Technology (ICT) systems that are critical for both the transmission of electricity and for electricity system operations. To protect our systems and information against a sophisticated and ever-changing threat, continuous and systematic work aligned to international best-practice standards is ongoing. To achieve this, we are working closely with other stakeholders in the sector and with national authorities.

One of our greatest challenges stems from the requirement for our sector to share data and connect systems between industry participants. This interconnected and shared risk drives the need for a continuous sector wide capability uplift.

The 2015 Cyber Security Strategy briefly acknowledges the importance of national critical infrastructure; however, it doesn't point to a specific strategy to improve its resilience or defensive posture. By providing a written submission for the current consultation process we seek to address this need.

Observations of the current state of cyber security practice

Security Ecosystem

- **NCPO and other Government Agencies:** The National Cyber Policy Office (NCPO), which is part of the Department of Prime Minister and Cabinet (DPMC), is responsible for New Zealand's cyber strategy. Responsibility for providing advice for crime, phishing, procurement, privacy and national security is shared across several government departments, representing some challenges due to the misalignment between strategy and the ability to respond.

- **NCSC & CSSIE:** The National Cyber Security Centre (NCSC), is part of the Government Communications Security Bureau (GCSB) and facilitates industry participants' participation in Security Information Exchange (SIE) forums. The forum relevant to our sector is the Control

Systems Security Information Exchange (CSSIE). This forum has agreed on common threat alert levels and incident response processes. It collaborates on exercises and actively engages in information sharing. These activities are largely driven by the bigger electricity sector participants and currently excludes other industries reliant on Industrial Control Systems (ICSs). While the NCSC facilitates the forum, it does not provide leadership. There is little visibility of or connection with other critical infrastructure ICS users e.g. water. NCSC's response capability is solely focused on attacks originating from nation state actors.

- **CERT NZ:** New Zealand's Computer Emergency Response Team (CERT NZ) has been in existence for just over a year and has a very wide mandate covering everyone in New Zealand, from individuals through to businesses. This is unlike the NCSC, which is focused on the most significant public and private sector organisations in NZ. CERT NZ provides advice and, in certain cases, basic assistance. It is a branded business unit within the Ministry of Business, Innovation and Employment (MBIE).

  The information CERT NZ currently provides is limited to email distribution lists and website updates, with the intent of providing automated threat information to organisations that can consume it. The information provided does not typically address ICS threats. The provision of threat intelligence from the organisation is expected to be of limited value to both national infrastructure and large organisations with an existing cyber response capability, due to the inherent risk aversion of government departments vis a vis releasing information that may have a commercial impact. The organisation does not provide a response capability to support New Zealand's businesses.

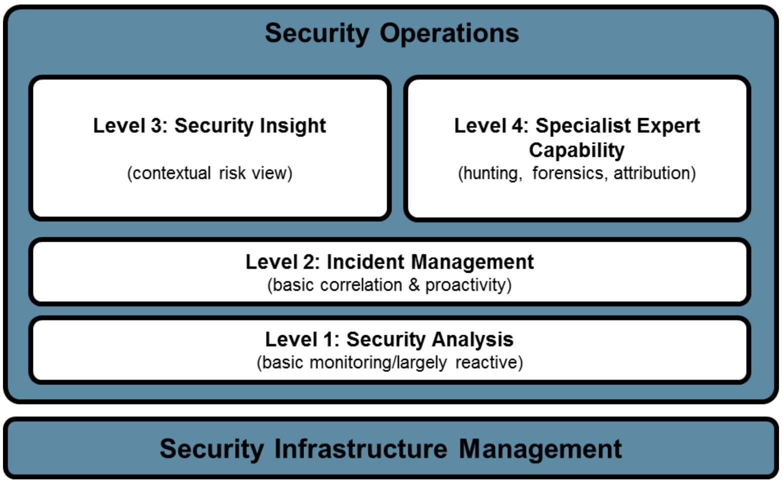
- **NZITF:** The New Zealand Internet Task Force is a non-profit organisation with the mission of improving New Zealand's cyber security posture. It is a forum based on mutual trust for debate, networking, information sharing, and collaboration on matters relating to the cyber security of New Zealand. Many of New Zealand's largest companies, government departments and tertiary education providers are members, along with a significant percentage of New Zealand's cyber security professionals. It is a good source of information concerning cyber issues and incidents in a New Zealand context. It is working on more sophisticated mechanisms for information sharing, but currently uses email distribution lists.

- **Commercial Managed Security Services:** A number of organisation in New Zealand provide managed security services including Security Operations Centres (SOC). All of these services cover the generic corporate IT environment and excludes specialised ICS capability. Importantly, all of these service offerings require some form of internal capability to respond to SOC alerts.

- **Organisational Security Operations Centres:** A number of New Zealand's larger organisations have their own SOCs. However, this capability appears more typically to be local resources that can respond to commercial, managed service provider alerts.

- **Individual skills and experience:** It is a universally accepted truth that there are limited number of skilled security specialists available in New Zealand and internationally. This results in most organisations having typically less capability and capacity than envisaged.

Security Capability Layers and Maturity
Potential solutions for the electricity sector are constrained by the ability of an organisation to respond to threat information or consume services. To assess the capability of organisations it is useful to understand that there are a number of capability layers that require some maturity in the related layers to be effective:


Security Operations
Level 3: Security Insight
(contextual risk view)
Level 4: Specialist Expert Capability
(hunting, forensics, attribution)
Level 2: Incident Management
(basic correlation & proactivity)
Level 1: Security Analysis
(basic monitoring/largely reactive)
Security Infrastructure Management

- **Security Infrastructure:** A well architected network with fit-for-purpose security devices and applications is the fundamental requirement for all organisations.

- **Level 1 - Security Analysis:** An alert level role. Analysts monitor the data feed, triage any security alerts and collect data and context in the event of an escalation to Level 2.

- **Level 2 - Incident Management:** Perform basic proactive correlation activities, using defined use cases and parameters to determine if a breach has occurred. Also responsible for the collection of data sets and the initial determination of the extent of systems compromised and provides support to Level 3 to do incident investigation and response.

- **Level 3 - Security Insight:** Takes the data feed and determinations from Level 2 to perform a deep-dive analysis of the incident, to determine steps to contain any breach and recover. Then works closely with Level 2 to implement remediation measures and commence recovery. Performs threat hunting within the internal environment. And, is responsible for providing a contextual risk view.

- **Level 4 - Specialist expert capability:** Performs reverse engineering, forensic analysis and completes attribution (source identification). Have a clear understanding of Advanced Persistent Threats (APTs).

The security capability of electricity sector participants varies based largely on their relative size which results in two segments:

1. **Small to Medium:** These organisations have comparatively little security capability and represent the majority (by number) of the sector. These organisations are typically under-equipped with security infrastructure and seldom have more than a few IT resources (who are unlikely to be security specialists). This segment is highly reliant on supporting organisations to provide threat intelligence and assistance in cases of compromise. The impact on New Zealand of a security compromise in one of these organisations is mostly restricted to smaller regions.

2. **Large:** The larger organisations have greater security capabilities by virtue of their size. This translates directly into security spend on services and infrastructure. There are a relatively small number of organisations in this segment and a wide range of capability ranging from having one security specialist to having a SOC capability (i.e. minimum of four specialists and commensurate infrastructure). Compromise of these organisations could significantly impact on the ability to maintain electricity supply to consumers.

These observations along with the assumption that other critical infrastructure sectors will be in a similar (or worse) position indicates that New Zealand’s critical infrastructure has significant areas of exposure that the National Cyber Security Strategy and Action Plan should have a role in addressing.

Potential Solutions

The potential solutions that should be considered for inclusion in a refreshed National Cyber Security Strategy and Action Plan are different for each of the segments of the electricity sector. However, in all cases the electricity sector and other sectors, which utilise ICS, would benefit from the development of an ICS CERT in a similar approach to that established in the US and Israel.

An ICS CERT capability would provide filtered threat intelligence, advice and support to the New Zealand critical infrastructure community in addition to the more generic threat intelligence and information provided through CERT NZ.

New Zealand requires a cyber response capability that can provide both proactive and reactive support to businesses, to fill the current void not covered by the nation state-actor focused NCSC. While this would ideally be government led it could also be provided through a private/public partnership.

The “small to medium segment” (above) also requires support in establishing a solid foundation in the security infrastructure base layer, as those organisations are typically small and will struggle to procure infrastructure and services at competitive rates. They may never be in a position to have a dedicated resource to respond to alerts generated by a commercially provided SOC or from CERT NZ. This segment is likely to benefit most from access to All-of-Government (AoG) providers utilising collective bargaining power.

The 'large segment' typically has a solid security infrastructure base along with one or more dedicated security specialists and can thus benefit from utilising a commercial SOC or having an internal capability. Threat information is obtained from non-New Zealand based entities either directly or indirectly through a local commercial SOC. The area currently absent in New Zealand is the provision of threat information relating to ICS in the New Zealand environment. The sector requires either the provision of this service through government or support in establishing the capability within New Zealand.

Yours sincerely

Cobus Nel
GM IST