

An update on industry arrangements for information security

23 September 2016

Note: This paper has been prepared for the purpose of the Security and Reliability Council (SRC). Content should not be interpreted as representing the views or policy of the Electricity Authority.

Background

The Security and Reliability Council (SRC) functions under the Electricity Industry Act 2010 (Act) include providing advice to the Electricity Authority (Authority) on reliability of supply matters.

Information security, in the context of the Authority's statutory objective, has potentially severe impacts on the promotion of reliability. As such, this is a topic that is within the SRC's scope to provide advice on.

An information paper describing the electricity industry's arrangements for information security (Information Paper) was provided to the 15 March 2016 meeting of the SRC.¹ Earlier versions of that Information Paper were presented to:

- the SRC on 22 October 2015
- the Smart Grid Forum on 9 February 2016
- the Control Systems Security Information Exchange (CSSIE) on 18 February 2016.

The SRC, at its 21 June 2016 meeting, requested "an update on cybersecurity-related matters at the 19 October 2016 SRC meeting." This paper provides the requested update.

Actions arising from the Information Paper

The Information Paper, and the associated cover paper, discussed four matters that the Authority planned to take further action on:

- clarifying the role of the Authority
- an information security exercise for the electricity industry
- a risk of domestic-scale controllable equipment being maliciously controlled
- an industry-wide risk assessment.

Clarifying the role of the Authority

The Information Paper noted that "The Authority may seek to establish a memorandum of understanding with NCSC [the National Cyber Security Centre], similar to what the Authority already has in place with the Commerce Commission, Ministry of Business Innovation and Employment and Financial Markets Authority. The purpose of the memorandum would be to agree on the respective roles and expectations for information sharing."

Authority staff subsequently determined that a memorandum with NCSC would be not be suitable as they do not have a regulatory or policy focus. Authority staff instead met with staff from the National Cyber Policy Office (NCPO). The NCPO is a part of the Department of Prime Minister and Cabinet (DPMC) and exists to "lead cyber security policy advice for government and to advise on the government's investment in cyber security activities."²

The NCPO and the Authority are likely to collaborate on communication of relevant information from and to the electricity industry. The NCPO is connecting Authority staff with contacts from other government agencies facing similar challenges to the Authority.

¹ The paper is available from <http://www.ea.govt.nz/development/advisory-technical-groups/src/meeting-papers/2016/15-march-2016/>

² From <https://www.dpmc.govt.nz/ncpo>

The Authority and the NCPO are unlikely to develop a memorandum of understanding. The parties will ensure there is mutual clarity about their respective roles and, wherever possible, do so in a transparent manner.

As discussed in paragraphs 2.15-2.34 of the Authority's Information Paper, there were already a number of governmental agencies with an interest in information security. The subsequent creation of a Computer Emergency Response Team (CERT) has added another agency to the mix: whether this improves or degrades the clarity of roles/objectives remains to be seen.

An information security exercise for the electricity industry

Members of the SRC, the Smart Grid Forum and the CSSIE were strongly in favour of the electricity industry undertaking an information security exercise to improve the industry's readiness for a cyber incident.

The Authority is unaware of any progress on such an exercise. Despite every indication that participation from the industry would be high, there is some inertia to be overcome for such an event to be organised. This appears to be because no individual organisation is responsible for organising it, despite an inherent collective responsibility. In the absence of a directive from senior industry management, information security practitioners appear likely to stay focussed on their own companies' needs, without considering the bigger picture and interdependencies with other industry participants.

The NCPO aims to run three cyber-security exercises every year. However, they are fully committed for at least the next 18 months so could not offer to lead the planning for an electricity industry exercise. However, the NCPO have offered to *assist* by advising the lead organiser.

A risk of domestic-scale controllable equipment being maliciously controlled

The Smart Grid Forum were particularly concerned about the emerging risk posed by consumer equipment being maliciously controlled in order to damage or collapse the power system.

The Authority subsequently asked the system operator to investigate how much controllable equipment (in MW) would need to be maliciously controlled to pose a credible risk to the power system. The system operator has undertaken some modelling of the power system and will attend the discussion of this agenda item to confidentially present the results of that modelling to the SRC.

An industry-wide risk assessment

The Smart Grid Forum and the CSSIE agreed that an industry-wide cyber-risk assessment be undertaken. The Authority noted at the time that the SRC's risk management framework could be used for such an undertaking.

The secretariat has been bearing this requirement in mind as it continues to develop the risk management framework.

Other developments since 15 March 2016

Three other relevant cybersecurity developments in New Zealand have occurred since the SRC's 15 March 2016 meeting:

- New Zealand's inaugural Cyber Security Summit
- details of CERT establishment announced
- PwC have initiated 'Insulator'.

New Zealand's inaugural Cyber Security Summit

New Zealand's inaugural Cyber Security Summit was held on 5 May 2016. The programme was designed to be of interest to senior industry leaders across the breadth of the economy. Actions arising from the workshop sessions at the Summit included:

- a project reference group has been set up to provide advice and guidance on content and certification options for the development of a Cyber Credentials scheme for small businesses by the end of 2016³
- a small business reference group will be established by the end of August 2016 to test the effectiveness of the Cyber Credentials scheme
- a public-private sector taskforce, involving participants from the workshop, will be set up by August 2016 to develop initiatives to build the cyber security workforce
- the NCPO will work with Connect Smart⁴ partners to extend the content of Connect Smart messages and develop new tools to help businesses improve their cyber security capability.⁵

Details of CERT establishment announced

At the time of the 15 March 2016 SRC meeting, the creation of a national CERT (a computer emergency response team) for New Zealand was known about. However, few details were available.

The Communications Minister Amy Adams has since announced that the CERT:

- has funding of \$22.2 million set aside. \$20 million of that is to fund four years of operating expenditure; \$2.2 million is to fund capital expenditure associated with start-up costs
- will initially be a separate unit within Ministry of Business, Innovation and Employment
- will start operating in the first quarter of 2017
- has an Establishment Advisory Board comprised of:
 - Michael Wallmannsberger (Wynyard Group), Chair
 - Sarah Burke (ANZ)
 - Jon Duffy (TradeMe)
 - David Eaton (Hewlett Packard Enterprise New Zealand)
 - Paul McKittrick (formerly with Government Communication Services Bureau)
 - Debbie Monahan (founder of Domain Name Commission)
 - Kendra Ross (Duo Ltd)
 - Rick Shera (Lowndes Jordan)

³ The Cyber Credentials scheme would enable small businesses to assure their customers that they are a reputable and trustworthy supplier, similar to the QualMark scheme achieves for accommodation businesses.

⁴ Connect Smart is "a partnership that promotes ways for individuals, businesses and schools to protect themselves online." The Connect Smart website (<https://www.connectsmart.govt.nz>) provides advice on safe and secure use of the internet by households, businesses and schools.

⁵ Information sourced from <https://www.connectsmart.govt.nz/events/summit-2016/> and <https://www.connectsmart.govt.nz/assets/Uploads/Summit-Report-FINAL.pdf>

- Adrian van Hest (Pricewaterhouse Coopers).⁶

PwC launched the 'Insulator' initiative

On 21 June 2016, Pricewaterhouse Coopers (PwC) launched the *Insulator* initiative by facilitating a training and networking event for energy industry professionals involved or interested in information security. The purpose of the initiative is to encourage collaboration and collective capability improvement across the New Zealand industry. PwC considers that New Zealand's size is both a strength and a weakness: we are small enough to be nimble and collaborate effectively, but lack the scale and sheer resources of most industrialised nations, so need to work together.

PwC found that the event was well-attended and that those attendees were highly-engaged and provided very positive feedback. As a result of the launch event, there are now plans for a meeting specifically for energy sector CIOs and other activity to develop industry capability and collaboration through the *Insulator* forum.

The SRC may wish to consider the following questions.

- | | |
|------------|---|
| Q1. | Does the SRC have any advice for how the industry can initiate an information security exercise? |
| Q2. | Does the SRC have any questions or suggestions for the system operator on the topic of maliciously-controlled consumer equipment? |
| Q3. | What further information, if any, does the SRC wish to have provided to it by the secretariat? |
| Q4. | What advice, if any, does the SRC wish to provide to the Authority? |

⁶ Information sourced from <http://www.cio.co.nz/article/599278/nz-government-allots-22-2m-computer-emergency-response-team-amy-adams/> and <https://www.beehive.govt.nz/release/cert-establishment-advisory-board-appointed>