Security and Reliability Council

# Progress against SRC actions relating to information security

28 March 2017

**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.

Breaches of information security can have potentially severe impacts on the reliability of electricity experienced by consumers. As such, this is a topic that is within the SRC's scope to provide advice on.

The SRC has previously received three papers on the topic of information security:

- paper describing the electricity industry's arrangements for information security (22 October 2015)
- updated version of the above paper (15 March 2016)[1]
- an update on cybersecurity-related matters (19 October 2016).

The SRC, at its 19 October 2016 meeting, created two actions relating to information security:

- The secretariat is to seek assurance from two major metering equipment providers (MEPs) about their cybersecurity posture and management of key risks.
- The secretariat is to present a proposal on potential ways that the industry can be encouraged to run an information security exercise.

This paper responds to those requested actions.

## Both major MEPs have agreed to present to the SRC

This action arose from a concern about a potential emerging risk posed by consumer equipment being maliciously controlled in order to damage or collapse the power system.

The secretariat has contacted the two largest metering equipment providers and asked them to consider responding to the SRC's request for assurance. Both have agreed to do so. Representatives of one of these MEPs will attend the SRC's 28 March 2017 meeting; the other will attend the 7 July 2017 meeting (due to scheduling difficulties for 28 March 2017). The MEPs have *chosen* to assist the SRC, though they are under no compunction to do so and this is a topic of considerable reputational and commercial sensitivity.

By agreement with both MEPs, the presentations will be provided in confidence. The Authority will not hold copies of the presentation slides. Slides will not be published or provided to SRC members.

The secretariat has tried to give the MEPs guidance about the level of information the SRC may be interested in to take some assurance from the MEPs' arrangements. If SRC members are not satisfactorily assured by the presentation, members should ask further questions.

The Institute of Directors of New Zealand publish a Cyber-Risk Practice Guide.[2] The secretariat has adapted recommended questions from that guide when formulating the below list of possible further questions:

- Does the MEP have a formalised framework for assessing risks, and is the risk of collapsing the power system documented within that framework?

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

[2] Available from https://www.iod.org.nz/Portals/0/Governance%20resources/Cyber-Risk%20Practice%20Guide.pdf

- Does the MEP receive adequate assurance that their outsourced providers and contractors have cyber controls, policies and process in place and monitored?
- Does the MEP have a response plan regarding cyber-attacks?
- Does the MEP choose to conform to any formal standards? (such as New Zealand's Voluntary Cyber Security Standards for Industrial Control Systems[3], or overseas standards)
- Does the MEP's Board have adequate access to cybersecurity expertise?

The SRC may prefer to defer giving any advice to the Authority on this topic until it has heard from both MEPs.

## Encouraging the industry to run an information security exercise

The secretariat has previously advised the SRC that despite every indication that participation from the industry would be high, there appeared to be nothing underway to organise an information security exercise. This was the catalyst for the SRC's action for the secretariat.

Since then, the secretariat has become aware that Pricewaterhouse Coopers (PwC) are attempting to initiate an event that will either directly satisfy the need for an exercise, or put the industry on a firm footing to be able to then plan an exercise. The secretariat is not concerned about whether this event is an "information security exercise" per se and considers that industry practitioners should set the scope and pace of events that coordinate a cross-section of the industry.

Separately, the Authority and Transpower have initiated planning for an exploratory meeting of relevant state sector agencies. This should help establish which agencies ought to be involved in an incident response and what further planning can and should be completed.

Accordingly, the secretariat has not developed "a proposal on potential ways that the industry can be encouraged to run an information security exercise." The secretariat will instead monitor further developments and report back to the SRC if the above developments fail to progress.

The SRC may wish to consider the following questions.

| | |
|---|---|
| **Q1.** | What further information, if any, does the SRC wish to have provided to it by the secretariat? |
| **Q2.** | What advice, if any, does the SRC wish to provide to the Authority? |

[3] Available from https://www.gcsb.govt.nz/assets/GCSB-Documents/NCSC-voluntary-cyber-security-standards-for-ICD-v.1.0.pdf