Security and Reliability Council

Cyber-security posture and management of key risks

28 July 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, at its 19 October 2016 meeting, created an action 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.

This paper responds to that requested action.

Both major MEPs 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 agreed to do so. Representatives of one of these MEPs attended (via video conference) and presented to the SRC's 28 March 2017 meeting. The other will attend the 28 July 2017 meeting. 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 are 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 Slides will not be published or provided to SRC members.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.[1] 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?
- 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[2], or overseas standards)
- Does the MEP's Board have adequate access to cybersecurity expertise?

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

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

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?