Security and Reliability Council

Industry arrangements for information security

Recapping the high-level arrangements relating to cyber and physical security of information and reviewing the Authority's next steps

2 March 2016

Note: This paper has been prepared for the purpose of discussion. Content should not be interpreted as representing the views or policy of the Electricity Authority.

Contents

Tables

Executive summary

The function of the Security and Reliability Council (SRC) is to provide advice to the Electricity Authority (Authority) on the performance of the electricity system and the system operator, and reliability of supply issues.

Information security is largely synonymous with cybersecurity, but is in fact broader and includes considerations of the physical security of information. Information security, in the context of the Authority's statutory objective, has potentially severe impacts on the promotion of reliability.

The SRC commented on an earlier draft version of the attached information paper at its 22 October 2015 meeting. That information paper is a high-level description of the electricity industry's arrangements with respect to information security. The piece of advice that the SRC gave which is most important in the context of this paper is that "the SRC will find out whether…[the view that the attached information paper is a complete and accurate high-level description is] shared by the Control Systems Security Information Exchange and the Smart Grid Forum."[1]

This paper:

- highlights the changes made since the Smart Grid Forum (Forum) and the Control Systems Security Information Exchange (CSSIE) reviewed the Authority's high-level description of information security arrangements
- seeks the SRC's advice on the next steps to be taken as a result of the Authority's discussions with various reviewers of the high-level description.

The key changes made since the SRC last saw the Authority's high-level description of the electricity industry's arrangements with respect to information security are:

- to account for announcements made since the Authority prepared its high-level description, such as the creation of computer emergency response team (CERT) and an update to *New Zealand's Cyber Security Strategy*
- to include more detail on the past work of the Internet Task Force
- to note that the Commerce Commission requires distributors to prepare asset management plans that demonstrate appropriate management of each distributor's assets

The Authority seeks the SRC's advice on whether:

- the SRC can encourage industry participants to undertake an information security desktop exercise and how best to coordinate this
- the actions the Authority has planned are suitable
- it is suitable that the Authority has no plans to take action on two areas of concern that were raised about industry arrangements.

[1] The SRC's complete advice is included in the correspondence for the 15 March 2016 meeting.

1 Introduction

1.1 Purpose of the paper

1.1.1 The Security and Reliability Council (SRC) has been appointed, in accordance with the Electricity Industry Act 2010 (Act), to provide independent advice to the Electricity Authority (Authority) on:

a) the performance of the electricity system and the system operator; and

b) reliability of supply issues.

1.1.2 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.

1.1.3 An information paper describing the electricity industry's arrangements for information security is attached as an appendix to this paper. Earlier versions of this high-level description were presented to:

a) the SRC on 22 October 2015

b) the Smart Grid Forum (Forum) on 9 February 2016

c) the Control Systems Security Information Exchange (CSSIE) on 18 February 2016.

1.1.4 The SRC's 2 December 2015 advice to the Authority included expectations that the SRC:

a) will find out whether the Forum and the CSSIE share the view that the high-level description is complete and accurate

b) wishes to continue to receive reporting about the security and reliability implications of information security as it comes to hand.

1.1.5 While the attached high-level description is a final version, it is not intended that the SRC need to (re)read this. The key changes since the SRC reviewed it are set out in section 2 below. The high-level description is provided in case SRC members want to see how the changes have been implemented or to reference any other part of that paper.

1.1.6 The primary purpose of this paper is to seek the SRC's advice on the next steps to be taken following the completion of the Authority's high-level description of industry arrangements for information security. The secondary purpose is to highlight the key changes to the high-level description since the SRC reviewed an earlier draft version in October 2015.

2 The high-level description has been improved in light of feedback received

2.1.1 The Forum and the CSSIE made the following suggestions for improvements to the high-level description.

Table 1: Suggestions from the Forum and the CSSIE and how these have been addressed

Suggestion	Party that suggested it	Where addressed in the high-level description
While the paper clearly described that physical security is an aspect of information security, that the paper is lacking much discussion of physical security.	Forum	Paragraphs 1.9, 2.6 and 2.7 add to this discussion
Since the paper was written, the Minister of Communications announced that New Zealand is establishing its own computer emergency response team (CERT).	Forum	Paragraphs 3.5 and 3.6 reflect this announcement
Since the paper was written, *New Zealand's Cyber Security Strategy* was updated. At the same time, an associated Action Plan and a National Cybercrime Plan were released for the first time.	Forum	Paragraph 2.15 reflects these changes.
The paper does not discuss the Commerce Commission's role. They require distributors to publish asset management plans that demonstrate appropriate asset management. The Authority understands that some distributors' asset management plans include high-level statements about their cybersecurity preparedness.	CSSIE	Paragraphs 2.26 and 2.27 reflect this information.
While the paper introduces the work of the Internet Task Force, it should mention its Computer Security Incident Response Team proof of concept[2] and its Coordinated Disclosure Guidelines.[3]	Forum	Paragraph 2.36 reflects this information.
The paper named the two dominant metering equipment providers but that "it may be useful to distinguish between meter data service providers and meter asset owners in Tables 1 and 2".	Forum	Footnote 14 to Table 1 assists readers with understanding there is a distinction and the numbers of organisations involved.

[2] More information from http://www.csirt.nz/

[3] Available from http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf

3 The Authority seeks the SRC's advice on the next steps

3.1.1 Aside from changes to the high-level description, the Authority has also received suggestions for other actions that may warrant further investigation. The following sections break these suggestions down into those the Authority intends to take at least some further action, and those where the Authority has no plans to take any action.

3.2 Additional suggestions that the Authority intends to take action on

An information security exercise appears to be beneficial

3.2.1 All three groups (SRC, Forum and CSSIE) were asked to comment on whether New Zealand electricity companies should be better involved in an information security exercise to test actual capabilities. All three groups were supportive of the concept and the CSSIE expressed a desire to directly participate in such an exercise.

3.2.2 The Smart Grid Forum and the CSSIE acknowledged that such an exercise can be a massive undertaking. Both groups seemed to favour a smaller, New Zealand-only desktop exercise as the best way to quickly learn and adapt. Subsequent exercises could be more complicated or involve coordination with other jurisdictions.

3.2.3 Authority staff consider industry interest is high enough such that the act of asking the question may have been sufficient to 'get the ball rolling'. Nonetheless, there is a distributed/collective responsibility that exists and this may be difficult to overcome. Therefore, Authority staff seek the SRC's advice on how best to encourage industry players to work together to develop a resourcing model to ensure the exercise happens in a timely manner.

The Authority will ask the system operator to attempt to quantify the risk of domestic-scale controllable equipment being maliciously controlled

3.2.4 The Forum devoted a significant portion of their time to a discussion about the new risks posed by domestic-scale controllable electrical equipment (such as solar photovoltaic panels, electric vehicles, smart meters, smart appliances). The concern expressed was that if the equipment were maliciously controlled and collectively cycled on and off for maximum disruption that the power system may collapse.

3.2.5 The Authority intends to ask the system operator to investigate how much controllable equipment (in MW) would need to be compromised in order to pose a credible risk to the power system. The Forum agreed that the present-day risk has low likelihood and low consequences due to the limited penetration of such equipment. As the potential consequence rises with growing penetration, so too does the likelihood of such a risk being targeted.

The Authority considers that cybersecurity risks to reliability can be captured within the SRC's risk management framework

3.2.6 The Forum suggested, and the CSSIE agreed, that an industry-wide risk assessment be undertaken. The Forum considered that the purpose of such an assessment would be "to prioritise the information security risks to the NZ electricity industry and identify those where cost of regulatory intervention is less than its benefits."

3.2.7 As the attached paper notes, the National Cyber Policy Office sets government cybersecurity strategy at an economy-wide level and the Authority's interpretation of its statutory objective means that Authority would be unlikely to regulate such an area. Even if this risk assessment

identified risks that fell within the Authority's remit, the Authority has a preference for non-regulatory solutions where possible.

3.2.8 Nonetheless, Authority staff see some benefits in a cybersecurity risk assessment as it may identify risks that are poorly managed and encourage better understanding of electricity industry interdependencies.

3.2.9 Authority staff consider that the development of the SRC's risk management framework provides a useful vehicle for completing such a risk assessment. Information security risks should show up as potential causes of risks to security and reliability.

3.3 Additional suggestions that the Authority has no plans to take action on

Industry participants are seeking mutual assurance that their counterparts are well prepared

3.3.1 The Forum and the CSSIE both expressed an interest in having better assurance of the preparedness of their industry counterparts. The Forum went so far as to suggest that there may be "national benefit in requiring all "participants"…to declare whether they comply with [the CSSIE's *Voluntary Cyber Security Standards for Industrial Control Systems*."

3.3.2 While the Authority would encourage owners of electricity control systems to comply with the CSSIE's standards it is wary of regulating this area (as noted in paragraph 3.2.7), especially overlaying a mandatory regime over a voluntary standard.

3.3.3 Authority staff consider that there are few barriers, if any, to the electricity industry obtaining the assurance it seeks through voluntary arrangements.

The design and configuration of information security protection for domestic-scale electrical equipment poses some concerns for the Forum

3.3.4 The Forum discussed its concerns about the information security of domestic-scale electrical equipment. They noted that:

a) individual household appliances don't warrant protection, but they do in aggregate. Manufacturers may not have strong incentives to harden their equipment against cyberattack

b) New Zealand will be a 'technology taker' with little leverage to influence global manufacturing standards

c) an information disclosure regime for household appliances (akin to the 'Energy Stars' system) would help consumers distinguish between products that meet or exceed information security standards, but would need to be complemented by consumer education

d) a mandatory certification regime for household appliances allows an expert body to set minimum information security standards for the protection of consumers

e) these are not matters that are within the Authority's regulatory powers

f) if the electricity industry considers it wants to be able to directly control the load associated with domestic-scale electric equipment then it needs to be exercised in a way that does not compromise the information security features of the equipment.

3.3.5 Authority staff acknowledge these concerns but have no plans to take any further action on the information security protection of domestic-scale equipment.

4 Questions for the SRC to consider

4.1.1 The SRC is asked to consider and provide advice on the following questions in the context of information security in New Zealand's electricity industry:

Q1.	Does the SRC have any recommendations on how best to encourage industry players to work together to develop a resourcing model to ensure an information security exercise happens in a timely manner?
Q2.	Does the SRC agree with the Authority's planned actions as set out in section 3.2?
Q3.	Does the SRC agree that the Authority should take no further action on the concerns set out in section 3.3?
Q4.	What further information, if any, does the SRC wish to have provided to it by the secretariat?
Q5.	What advice, if any, does the SRC wish to provide to the Authority?

Electricity industry arrangements for information security

An overview of arrangements relating to cyber and physical security of information

Information paper

8 March 2016

Market Services

Executive summary

This paper provides a high-level description of the electricity industry's arrangements with respect to information security. Information security is largely synonymous with cybersecurity, but is in fact broader and includes considerations of the physical security of information.

The Electricity Authority (Authority) is an independent Crown entity established with the purpose of promoting competition in, reliable supply by, and the efficient operation of the electricity industry for the long-term benefit of consumers.

Information security, in the context of the Authority's statutory objective, has potentially severe impacts on the promotion of reliability. Accordingly, the Authority is interested in understanding whether industry information security arrangements provide for an efficient level of reliability.

Naturally enough, the scope of any one industry participant's information security activities tends to be limited by the benefits that can accrue to their own organisation. Nonetheless, there are a wide variety of industry groups, not-for-profits, academics and government agencies with an interest in improving New Zealand's information security outcomes. In general, these groups have an economy-wide scope rather than looking solely at the electricity industry or even the energy sector.

The Authority thanks the following groups for their valuable feedback on different versions of this paper:

- The Security and Reliability Council (SRC). The function of the SRC is to provide advice to the Authority on the performance of the electricity system and the system operator, and reliability of supply issues.
- The Smart Grid Forum. The Forum's objective is to advance the development of smart electricity networks in New Zealand through information sharing and dialogue, supported by analysis and by focussed work-streams where these are considered to be appropriate.
- The Control Systems Security Information Exchange (CSSIE). The CSSIE are a large group of information security practitioners with representation from New Zealand's electricity lines businesses, generators, retailers and metering companies.

Thanks to the feedback received, the Authority considers this paper to be a complete and accurate high-level description of the information security arrangements of New Zealand's electricity industry. This paper is intended as a local snapshot only: no international context is included and the content is likely to become increasingly dated with time.

Contents

Tables

Figures

1 Introduction

Purpose of the paper

1.1 Information security, in the context of the Authority's statutory objective, has potentially severe impacts on the promotion of reliability.

1.2 The purpose of this paper is to develop a complete and accurate high-level description of the information security arrangements in New Zealand's electricity sector.

1.3 A high-level description of the arrangements in New Zealand is intended to be a first step that can be used in future to enable insight through:

(a) international comparisons

(b) identification of any gaps in responsibility that could lead to inefficiently unreliable supply to consumers

(c) identification of difficulties with interactions between different types of organisations.

1.4 The Authority values the CSSIE's perspective as a group of information security practitioners and appreciates any assistance or advice it can offer.

Information security is broader than cybersecurity

1.5 Information security is, for the purposes of this paper, taken to be an umbrella term for the activities of an organisation that are intended to identify, protect and restore its information. More specifically, the Authority's interest is limited to the activity of any industry participant that could have significant ramifications for consumers.

1.6 Other definitions of information security exist, such as:

> "…the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical)." [1]
>
> "Although sometimes described as cyber security, Information security is considered a higher level of abstraction than cyber security relating to the protection of information regardless of its form (electronic or physical). The accepted definition of information security within government is: "measures relating to the confidentiality, availability and integrity of information"." [2]
>
> "…to protect and preserve the confidentiality, integrity, and availability of information. It may also involve protecting and preserving the authenticity and reliability of information and ensuring that entities can be held accountable." [3]

1.7 In summary, information security:

(a) is a discipline in its own right that transcends the electricity industry, though it allows for industry- or organisation-specific requirements

---

1 From Wikipedia - https://en.wikipedia.org/wiki/Information_security

2 From paragraph 1.1.29 of the *New Zealand Information Security Manual* - http://www.gcsb.govt.nz/assets/GSCB-NZISM/NZISM-MAY-2015-v2.3.pdf

3 From Praxiom Research Group Limited's *ISO 27000 InfoSec Definitions Translated Into Plain English* - http://www.praxiom.com/iso-27000-definitions.htm

(b) is often used synonymously with cybersecurity[4]

(c) has an extensive body of literature largely focussed at the level of an individual organisation

(d) includes the physical protection of assets and premises to the extent that this can compromise an organisation's information

(e) requires attention and endorsement at each organisation's governance level

(f) operates best within a risk-based framework to set organisational goals and policies

(g) integrates with incident management and business continuity management

(h) is not 'just an IT thing' that can operate successfully as an isolated corporate function of an organisation

(i) requires communication and operations management to ensure that *people* comply with policies and achieve an organisation's goals.

Many aspects of information security are similar around the world

There are a handful of different types of threat actors

1.8 The array of possible system vulnerabilities is virtually limitless, but it tends to be a handful of the same types of actors who would seek to exploit vulnerabilities. These threat actors (sometimes known as adversaries) have different motivations, different sophistication/resources, and different frequency of cyberattacks as illustrated in Figure 1. At either end of the spectrum are:

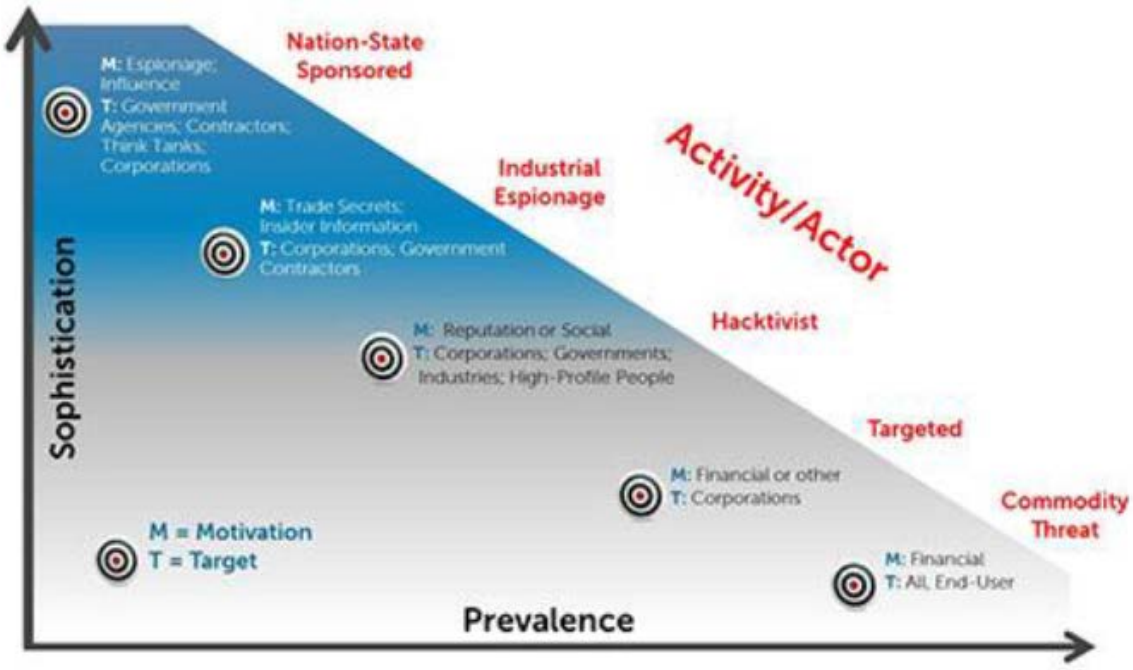
(a) hordes of 'script kiddies' who seek to test their skills and gain notoriety amongst peers by demonstrating their 'power'

(b) scores of nation-states that have the resources and sophistication to plan and execute the most elaborate cyberattacks against a select range of targets.

1.9 Information security breaches can also be self-inflicted without the help of any threat actor. This would usually involve some breach of the organisation's policies such as the active sending of important information to unintended recipients or leaving information (paper or digital records) in public places.

[4] 'Cybersecurity' definitions vary even more than 'information security'. Gartner Inc define cybersecurity as encompassing "…a broad range of practices, tools and concepts related closely to those of information and operational technology security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries." - http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

Figure 1: An overview of threat actors



Source: Dell Secureworks

Notes: 1. From http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat/

A substantial portion of intrusions involve insiders

How these threat actors attack varies, but one way of analysing the attacks is by examining whether attacks were executed by outsiders acting alone, involved malicious insiders or insiders inadvertently assisting the threat actor. Figure 2 presents IBM's illustration of this analysis.

Figure 2: Analysis of global 2014 cyberattacks by intentional involvement of insiders

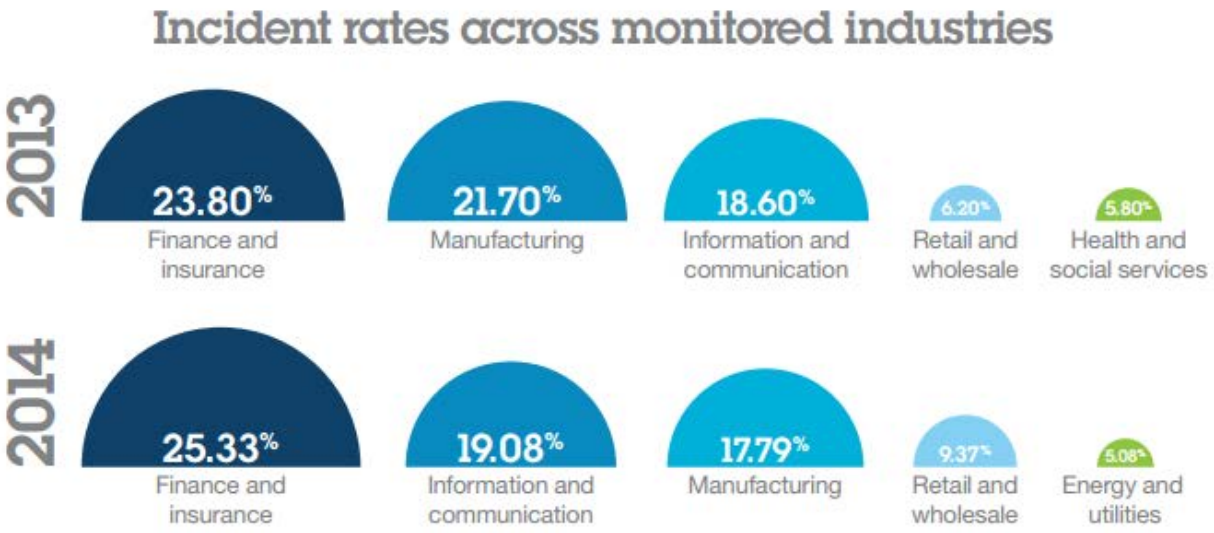
Source: IBM's 2015 Cyber Security Intelligence Index

Notes: 1. From http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

In 2014, just over 5% of incidents targeted the energy and utilities sector

1.11 The preferred targets of threat actors can change from year to year, but the finance and insurance sector is consistently the most-targeted sector.

Figure 3: Incident rates across monitored industries



Source: IBM's 2015 Cyber Security Intelligence Index

Notes: 1. From http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03073usen/SEW03073USEN.PDF

The impact of information security breaches is sizable

1.12 The annual global cost of cybercrime and cyberespionage has been estimated at over $400 billion (USD) by security firm McAfee in 2014.[5] Applying McAfee's estimated losses of 0.9% of New Zealand's gross domestic product indicates an annual cost of $2.1 billion (NZD).[6]

1.13 Symantec's *Norton Cybersecurity Insights Report* used survey results to estimate that $257 million (NZD) was lost to cybercrime in New Zealand in the year to August 2015.[7]

Real-life situations highlight why threat actors choose their targets and how they execute their cyberattack

1.14 In order to draw the above observations together into tangible situations, it is useful to consider some real-life situations.

(a) In June 2010, a security company identified a particularly sophisticated computer worm that came to be known as Stuxnet. The degree of sophistication and the apparent intended target (Iran's uranium enrichment facilities at Natanz) led to speculation that Stuxnet was a

5 From http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime2.pdf

6 Based on Statistics New Zealand's official estimate of New Zealand gross domestic product as $240 billion (NZD) for the June quarter of 2015.

7 Available from https://us.norton.com/norton-cybersecurity-insights-report-newzealand?inid=hho_norton.com_cybersecurityinsights_p3_seectryrpts

product of the United States and Israeli governments. Stuxnet reportedly destroyed about a fifth of Iran's nuclear centrifuges.[8]

(b) In March 2007, Idaho National Laboratory demonstrated the Aurora vulnerability by staging a cyberattack on a synchronised 2.25MW diesel generator that they bought for that purpose. By exploiting weaknesses in an associated control device, the researchers destroyed the generator by opening and closing breakers to put the machine out of synchronisation.[9]

(c) On 23 December 2015, 80,000 Ukrainian electricity users experienced a six-hour power outage that was caused by unauthorised switching of circuit-breakers. The unauthorised switching was caused by BlackEnergy, a malware that infiltrated utility networks via a corrupted Microsoft Word email attachment. No organisation claimed responsibility for the attack, though both the Russian state and Russian hacker groups have been blamed.[10]

(d) In June 2014, the popular newsfeed service Feedly suffered a distributed denial of service (DDoS) attack that incapacitated their service for over three days. The attackers sought to extort money from Feedly in exchange for ending the attacks.[11]

(e) In 2013, a small New Zealand business received emails threatening to disable their business unless funds were paid – a cyberattack known as 'ransomware'. When no funds were paid, the threat actor compromised the business' servers and installed malware that encrypted their data, causing the business to lose access to its systems. The business took several days to become operational again and lost some data when they restored from historic backups.[12]

2 New Zealand's electricity industry arrangements

Electricity industry participants can protect themselves individually, but face some collective risks

2.1 The security of information in the electricity industry is directly dependent on the actions of the following types of organisations/people and their agents:

(a) consumers (large or small users, or load aggregators)

(b) metering equipment providers

(c) distributors

(d) generators

(e) retailers

---

8 As reported by The New York Times - http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0

9 From https://en.wikipedia.org/wiki/Aurora_Generator_Test, a video of the demonstration can be downloaded from https://muckrock.s3.amazonaws.com/foia_files/aurora_high_res.wmv

10 From http://www.newsweek.com/russian-hackers-shut-ukraine-power-grid-415751 and http://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112

11 More information from www.forbes.com/sites/jaymcgregor/2014/07/28/the-top-5-most-brutal-cyber-attacks-of-2014-so-far

12 Page 8 of the National Cyber Security Centre's *2013 Incident Summary* - http://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-incident-statistics-for-year-to-December-2013-final.pdf

(f) market operation service providers (such as the registry manager or the system operator)

(g) transmission operator (Transpower).

2.2 There are other entities that influence the actions of the above organisations/people, but do not typically hold critical electricity industry information:

(a) state sector agencies

(b) industry groups

(c) not-for-profit groups.

2.3 While information security is practiced at the level of the each individual organisation or person, these practitioners have very different incentives, capabilities and externalities. For example:

(a) domestic electricity consumers rarely consider the security of their information, and traditionally their actions have had no potential impact on anyone but themselves

(b) generators have strong incentives to protect their generation control systems that enable their revenue streams; though the downstream impacts on consumers could be much greater if several generation plant are taken offline in an coordinated cyberattack.

2.4 Asset ownership usually provides for clear delineation of responsibility for information security. However, responsibility only extends to each organisation's information and assets whereas the downstream impact is a cost borne by consumers (in the case of lessened reliability) and competitors (in the case of industry-wide reputational damage). This situation is not peculiar to incidents caused by cyberattacks – any operational incident affecting critical infrastructure can have downstream reliability or reputational impacts not borne by the owner of the critical infrastructure.[13]

2.5 The scope of what is considered critical infrastructure has broadened over time as organisations become more dependent on technology and inter-dependent on each other and market systems.

2.6 Organisations with field assets (as opposed to office-based assets like workstations and servers) have extra layers of critical infrastructure to protect. The field assets need physical protection and the associated control systems and communications networks need physical and electronic protection.

2.7 The need to physically secure information associated with field assets is well-aligned with the need to physically secure assets for commercial and health and safety reasons. To protect against risks such as metal theft and accidental electrocution, key field assets (generators, substations, SCADA terminals) invariably need barriers (locked doors, fences) to restrict access. Other physical security measures such as site monitoring (CCTV) and incident response plans are less ubiquitous, but also well-aligned with cybersecurity needs.

2.8 Electricity field assets are particular to this industry, whereas office-based assets are homogenous across industries. Table 1 illustrates the different types or organisations and their protection requirements.

[13] Though causers of under-frequency events face an event charge of $1,250/MW under clauses 8.60-8.66 of the Code.

Table 1: Electricity industry organisation types and their asset types for protection

Organisation type	Estimate of key organisations involved	Critical office-based assets such as servers and workstations	Critical field assets and associated control systems and communications networks
Transmission	One (Transpower)	Yes	Yes, such as HVDC and SCADA
Generation	About six owners of large-sized generation, dozens of owners of medium-sized	Yes	Yes, such as generation plant and control systems
Distribution	About 30 local networks, plus scores of embedded networks	Yes	Yes, such as protection systems and SCADA
System operator	One (Transpower)	Yes	Yes, such as SCADA and communications networks
Other market operation service providers	Eight (ranging from a very high availability service with the registry to annual processing of the extended reserve manager)	Yes	No
Metering	Two[14] (Advanced Metering Services and Metrix)	Yes	Yes, metering assets and communication networks
Retailing	23 parent companies operating 28 brands	Yes	No
Consumer	About two million ICPs	No	Yes, such as home energy management systems, small-scale distributed generation, any controllable loads

[14] These two metering equipment providers (MEPs) provide services to over 95% of the smart metering market. There are about another 10 MEPs and an even more diverse range of owners of metering equipment.

Industry groups provide important information sharing

2.9 The most important electricity industry group for information security in New Zealand is the CSSIE. The CSSIE is about five years old and serves to enable candid exchange of information among trusted industry peers. CSSIE is facilitated by the National Cyber-Security Centre, whose role is discussed further from paragraph 2.16.

2.10 The CSSIE, as the name suggests, was brought together to provide focus on the critically important control systems found in the bulk-supply side of the electricity industry. As such, the group has had representatives from Transpower, gentailers and distributors. This historic focus is highlighted in Table 2 below.

Table 2: Assets for protection, with CSSIE's historic focus highlighted in green

Organisation type	Critical office-based assets such as servers and workstations	Critical field assets and associated control systems and communications networks
Transmission	Yes	Yes, such as HVDC and SCADA
Generation	Yes	Yes, such as generation plant and control systems
Distribution	Yes	Yes, such as protection systems and SCADA
System operator	Yes	Yes, such as SCADA and communications networks
Other market operation service providers	Yes	No
Metering	Yes	Yes, metering assets and communication networks
Retailing	Yes	No
Consumer	No	Yes, such as home energy management systems, small-scale distributed generation, any controllable loads

2.11 More recently, metering representatives have joined the CSSIE. The introduction of 'smart' meters into New Zealand opens up a new avenue for potential cyberattack.

2.12 The CSSIE developed a set of voluntary guidelines: *Voluntary Cyber Security Standards for Industrial Control Systems*. The guidelines are intended to "…enhance the cyber security of electricity sector industrial control systems. The objective is to provide a cyber security framework to ensure the reliable operation of the New Zealand electricity system."[15] The guidelines are based on standards developed by the North American Electric Reliability Corporation (NERC), though they've been designed for application in New Zealand.

[15] From http://www.cigre.org/What-is-CIGRE and http://www.cigre.org.nz/aboutnznc.html

2.13 The International Council for Large Electric Systems (CIGRE) is an international body with a New Zealand National Committee. The purpose of CIGRE is to promote collaboration amongst electricity industry experts. An advantage of CIGRE is its size and access to international insights. In the context of information security, where it is especially valuable to target the sharing of information among peers that are trusted not to repeat it publically, CIGRE may not be ideally placed to coordinate this discrete level of information sharing.

2.14 The International Electricity Infrastructure Assurance Forum (IEIA) is an international public-private partnership open to participation from Australia, Canada, New Zealand, the United Kingdom and the United States. The purpose of the IEIA is to enhance protection of electricity infrastructure and stimulate active involvement of government and private participants. The IEIA has some of the advantages of CIGRE through limited international involvement with some of the benefits of CSSIE through higher trust and a more discrete forum.

The state sector has a variety of agencies with interests in information security ranging from direct to oblique

The National Cyber Policy Office sets government strategy for cybersecurity

2.15 The National Cyber Policy Office (NCPO) is the lead agency for setting cybersecurity policy for the New Zealand government.[16] As part of the Department of Prime Minister and Cabinet (DPMC), the NCPO is well placed to keep abreast of the intelligence agencies that report through DPMC. The NCPO's key activities are:

(a) ongoing development of *New Zealand's Cyber Security Strategy* (launched in 2011, updated in 2015) and associated *Action Plan*[17]

(b) contributing to, and publishing the *National Plan to Address Cybercrime* (launched in 2015)[18]

(c) leading international engagement on cybersecurity

(d) leading the ConnectSmart partnership that aims to "promote ways for individuals, businesses and schools to protect themselves online".[19]

The National Cyber Security Centre has the expertise and economy-wide ambit to take the lead operational role for cybersecurity

2.16 The National Cyber Security Centre (NCSC) is the lead government agency for operational management of cybersecurity in any New Zealand industry. The NCSC is part of the Government Communication Services Bureau (GCSB). The NCSC describe their purpose as "to protect government systems and information, to plan for and respond to cyber incidents, and to work with providers of critical national infrastructure to improve the protection and computer security of such infrastructure against cyber-borne threats."[20]

2.17 As discussed in paragraphs 2.9-2.12, the NCSC works alongside industry representatives to facilitate the effectiveness of the CSSIE, though they also facilitate security information exchanges in other New Zealand industries.

---

16 More information from http://www.dpmc.govt.nz/ncpo

17 Available from http://www.dpmc.govt.nz/dpmc/publications/nzcss

18 Available from http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-cybercrime-plan-december-2015.pdf

19 More information from https://www.connectsmart.govt.nz/

20 From http://www.ncsc.govt.nz/about-us/

2.18 NCSC has a monitoring role that includes the publication of aggregated statistics about the number and type of known cyberattacks. However, its monitoring activities do not presently extend to detailed information assurance processes (such as audits or compliance reporting).

The Authority's interest is promoting reliable supply of electricity for the long-term benefit of consumers

2.19 Information security, in the context of the Authority's statutory objective, has:

(a) little impact on the promotion of competition

(b) potential severe impact on the promotion of reliability

(c) some impact on the promotion of efficient operation.

2.20 Looking solely at the Authority's statutory objective without any context, information security appears to be well within the Authority's role to regulate. However, paragraph A.60 of the Authority's I*nterpretation of the Authority's statutory objective* sheds more light on the Authority's role.

> "In particular, the Authority believes that policies to address externalities arising generally from industry and consumer activity that is broader than electricity industry-related activity do not fall within the scope of the Authority's functions."[21]

2.21 The Authority may seek to establish a memorandum of understanding with NCSC, 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.

2.22 Information security is a fast-paced, rapidly evolving discipline. Legislation that prescribes in detail how information must be protected, or sets outcome-based performance standards will quickly be outdated.

2.23 For these reasons, the Authority is highly unlikely to consider using its legislative powers to promote information security. The Authority's role could include helping to coordinate, facilitate or monitor information security preparations.

2.24 While the Authority has been comfortable taking a back seat given the roles and responsibilities of NCPO and NCSC, it is fully cognisant that it has a governance responsibility toward the nine market operation service providers (MOSPs):

(a) Transpower in its capacity as system operator and financial transmission rights (FTR) manager

(b) NZX in its capacity as reconciliation manager, pricing manager, clearing manager, wholesale information trading system (WITS) manager and extended reserve manager

(c) Jade Software Corporation as the registry manager

(d) the Authority as the market administrator.

2.25 While each MOSP has primary operational responsibility for the information security of their service, the Authority has a governance responsibility. To this end, the Authority has:

(a) been updating MOSP contracts to enable best practice information security and allow flexibility for adaptation as the security environment changes

[21] Available from http://www.ea.govt.nz/about-us/strategic-planning-and-reporting/foundation-documents/

(b) started a regime of information security audits of MOSPs to provide an independent and expert review of each MOSP's preparations.

The Commerce Commission regulates the quality of supply by distribution businesses

2.26 The Commerce Commission is an independent Crown entity whose responsibilities include the regulating of monopoly business (such as electricity distribution businesses) under the Commerce Act 1986. It applies price-quality regulation to distributors which means their aggregate regulated revenue is capped and they have quality targets to meet.

2.27 Furthermore, the Commerce Commission requires distributors to create asset management plans and for these plans to provide information that shows the distributor is managing assets appropriately. The Authority understands that some distributors' asset management plans include high-level statements about their cybersecurity preparedness.

There are many other state sector agencies with an interest in information security

2.28 There are a handful of other government agencies with a role to play in information security. They are set out below.

2.29 The members of the New Zealand Intelligence Community[22], namely:

(a) The New Zealand Security Intelligence Service (NZSIS). Their core role is intelligence gathering and evaluation, though they do also provide advisory services to government security staff.[23] NZSIS manage the *Protective Security Requirements* that are security best-practice.

(b) The Government Communication Services Bureau (GCSB). Through the NCSC, as discussed from paragraph 2.16, the GCSB has a cybersecurity function that interacts with government and private sector organisations. The GCSB's non-NCSC functions are largely focussed offshore and result in provision of foreign intelligence to government decision-makers. However, the GCSB are also responsible for the *New Zealand Information Security Manual* (NZISM) that serves as a practitioner's handbook on information assurance and information systems security.[24]

(c) The National Assessments Bureau (NAB). The NAB's role is comparatively narrow and is to "provide assessments to assist decision makers on events and developments relevant to New Zealand's national security and international relations."[25]

2.30 The Government Chief Information Officer (GCIO) is part of the Department of Internal Affairs (DIA). The GCIO's responsibilities include:

(a) setting policy and standards for government information and communications technology (ICT)

(b) improving government ICT capability

(c) providing formalised assurance of government ICT.

2.31 Apart from the GCIO's influence on the Authority, its activities do not otherwise impact on the electricity industry. The GCIO influences the Authority (and other public agencies) by requiring

---

22 More information from http://www.nzic.govt.nz/

23 More information from http://www.nzsis.govt.nz/about-us

24 Available from http://www.gcsb.govt.nz/news/the-nz-information-security-manual

25 From http://www.dpmc.govt.nz/nab

that "information…must be secure" and recommending that agencies *should* "follow applicable security guidelines".[26] In practice, unless a standard is not applicable or a better alternative is available, this means following:

(a) the *Protective Security Requirements*

(b) the NZISM.

2.32 The New Zealand Police have a National Cyber Crime Centre (NC3) dedicated to dealing with online crime. NC3 provide the specialist skills to be able to detect and monitor cybercrime, which complements the more general requirements of the New Zealand Police.

2.33 The Privacy Commissioner has several functions, but the most relevant for the electricity sector are the investigation of privacy breaches and development of Codes of Practice. Meeting best practice and legislative requirements for the protection of individuals' privacy is a major motivation for most electricity industry participants. The legislative requirements, and the existence and role of the Privacy Commissioner, are set out in the Privacy Act 1993.

2.34 The National Infrastructure Unit (NIU). The NIU takes advice from the National Infrastructure Advisory Board to formulate and monitor a national infrastructure plan. The most relevant goal from the NIU's current *Thirty Year New Zealand Infrastructure Plan* is that:

> "Our electricity networks will be more resilient. This will be achieved through...Protection of New Zealand's energy infrastructure in order to avoid vulnerabilities and disruptions to service, including cyber risks where advice has been developed in conjunction with the electricity sector for the protection of industry control systems."[27]

There are a variety of not-for-profit organisations that seek to promote security online

2.35 There are several not-for-profit organisations with important roles to play in cybersecurity generally, though none have any particular focus on the electricity sector.

2.36 The New Zealand Internet Task Force (NZITF) is a membership-based forum of trusted industry, government and academia personnel with a mission of improving New Zealand's cybersecurity posture. The activities of the NZITF include:

(a) training and information sharing[28]

(b) continued development of the *Coordinated Disclosure Guidelines* it published in October 2014[29]

(c) developing a Computer Security Incident Response Team as a proof-of-concept for a national Computer Emergency Response Team (CERT).[30]

2.37 Netsafe is a membership-based organisation that seeks to promote "confident, safe and responsible use of online technologies." There are a wide array of publications and initiatives promulgated by Netsafe, but the two most relevant to information security are set out below.

---

26 From the *Records Management Standard* issued under the Public Records Act 2005

27 Page 60 of the *30 Year New Zealand National Infrastructure Plan* (2015) - http://www.infrastructure.govt.nz/plan/2015/nip-aug15.pdf

28 More information from http://www.nzitf.org.nz/

29 Available from http://www.nzitf.org.nz/pdf/NZITF_Disclosure_Guidelines_2014.pdf

30 More information from http://www.csirt.nz/

(a) Security Central provides basic and useful security advice for individuals and small businesses. It reinforces simple security messages that are sufficient to protect users from the majority of scams and exploits.[31]

(b) The Orb provides a simple and safe way for the public to report concerns about online incidents. These concerns are relayed to relevant partner organisations, such as New Zealand Police for online crimes and NCSC for cyberattacks.[32]

2.38 The New Zealand Institute of Directors "promotes excellence in corporate governance, represents directors' interests and facilitates their professional development through education and governance training".[33] As part of that role, they have published a Cyber-Risk Practice Guide to assist Board directors with providing appropriate governance for their organisations.[34]

2.39 The New Zealand Security Association represents the interests of the security industry. While this representation is predominantly in the aspects of physical security, it also runs a sub-group called the New Zealand Security Information Forum (NZSIF). NZSIF seeks to promote expertise in information security among its membership and in the general community.[35]

2.40 Waikato University is establishing a reputation as the leading New Zealand university for the study and research of cybersecurity. Waikato University:

(a) offer New Zealand's first Masters of Cyber Security qualification to students

(b) have established the Cyber Security Researchers of Waikato group (CROW) to conduct research relating to data security[36]

(c) run the annual New Zealand Cyber Security Challenge in which teams meet to compete to solve a series of cybersecurity challenges that are revealed on the day of competition[37]

(d) has an award-winning expert (Dr Ryan Ko) leading its cybersecurity research and education.[38]

2.41 InternetNZ is a membership-based society that seeks to "promote the Internet's benefits and uses and protect its potential."[39] A large part of their activity relates to domain names and is performed its subsidiaries: New Zealand Registry Services and the Domain Name Commission. More pertinently to information security, InternetNZ also supports Netsafe in performing its functions.

---

31 More information from http://www.securitycentral.org.nz/

32 More information from http://www.theorb.org.nz/

33 From https://www.iod.org.nz/About-us

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

35 More information from http://security.org.nz/nzsif/

36 More information from https://crow.org.nz/

37 More information from https://cybersecuritychallenge.org.nz/

38 From http://www.waikato.ac.nz/news-events/media/2015/award-for-cyber-security-head

39 From https://internetnz.nz/about/our-vision

3 The global and local information security environment will continue to change

Information security best practice has a history of continual evolution

3.1 According to Da Veiga and Eloff, information security has undergone three phases in its evolution:

(a) phase one was when information security was regarded as a function of technical departments

(b) phase two was when information security got governance oversight and became better integrated into organisational management through the adoption of goals and policies

(c) phase three was when information security became recognised as an enterprise-wide activity, with every person an important link in the security chain.[40]

3.2 At the technical level, the historic approach of a reactive perimeter defence has morphed into providing a risk-based 'defence-in-depth' approach that provides layers of defence and includes offensive capabilities.

3.3 This type of general evolution of information security as a discipline will continue regardless of what happens in New Zealand's electricity industry. However, some changes in the electricity industry will create new risks and threats to be actively managed within organisations' information security governance frameworks. Some examples of these types of changes are:

(a) new supply-side technology like smart meters and transmission/distribution automation

(b) new demand-side technology like home automation, greater load control, more distributed generation, more electric vehicles and the growing 'internet of things'

(c) new ways of servicing consumers.

3.4 As these new technologies proliferate, the likelihood and consequence of an attack from this emerging threat vector increases. Quantifying the take-up of these different technologies, and what that means in terms of potential impact on the power system, will therefore be of increasing importance.

New Zealand will establish its own Computer Emergency Response Team

3.5 The Minister of Communications' press release of 10 December 2015 announced the decision to establish a CERT for New Zealand, similar to what other jurisdictions operate.[41]

3.6 The CERT will act as a single point of contact for New Zealand individuals, firms and government agencies to receive direct assistance with a cybersecurity incident. This could lead to better coordination within New Zealand agencies, but also with overseas partners. As a major cyberattack could stretch the time and expertise capacity of New Zealand personnel, increasing that capacity and having access to overseas experts will be valuable.

New Zealand should establish regular information security exercises

3.7 Overseas jurisdictions commonly run information security exercises to test the readiness of industry operators. Some examples are:

---

40 From *An Information Security Governance Framework* written by A. Da Veiga and J.H.P Eloff and published in *Information Systems Management* (24:361-372, 2007)

41 More information from http://www.beehive.govt.nz/release/cyber-security-strategy-safeguards-nz-economy

(a) Cyber Storm, a biennial exercise run by the United States Department of Homeland Security since 2006[42]

(b) Cyber Europe, a biennial exercise run by the European Union Agency for Network and Information Security.

3.8 The groups that the Authority engaged with to review this paper were, in principle at least, in favour of New Zealand's electricity industry coordinating or participating in an information security exercise. The lack of a single organisation with the clear responsibility for planning and operation of such an exercise appears to be a key reason why such an exercise has not been run since approximately 2010. Industry stakeholders wishing to participate in such an exercise will need to establish a resourcing model to facilitate it.

[42] More information available from http://www.dhs.gov/cyber-storm-securing-cyber-space

Glossary of abbreviations and terms

Act	Electricity Industry Act 2010
CERT	Computer Emergency Response Team
CIGRE	International Council for Large Electric Systems
CROW	Cyber Security Researchers of Waikato
CSSIE	Control Systems Security Information Exchange
DDoS	Distributed denial of service
DIA	Department of Internal Affairs
DPMC	Department of Prime Minister and Cabinet
FTR	Financial transmission rights
GCIO	Government Chief Information Officer
GCSB	Government Communication Services Bureau
ICT	Information and communications technology
IEIA	International Electricity Infrastructure Assurance Forum
MOSP	Market operation service provider
NAB	National Assessments Bureau
NC3	National Cyber Crime Centre
NCSC	National Cyber Security Centre
NCPO	National Cyber Policy Office
NIU	National Infrastructure Unit
NZIC	New Zealand Intelligence Community
NZISM	New Zealand Information Security Manual
NZSIF	New Zealand Security Information Forum
NZSIS	New Zealand Security Intelligence Service
SRC	Security and Reliability Council
WITS	Wholesale information trading system