Security and Reliability Council

# Industry arrangements for information security

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

22 October 2015

**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

## Figures

## 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.

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.

Information security, in the context of the Authority's statutory objective, has potentially severe impacts on the promotion of reliability. Accordingly, the Authority Board requested that the SRC consider information security arrangements.

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.

This paper does not seek to draw conclusions from the high-level description of the arrangements. The high-level description and the questions posed for the SRC are a way of holding a mirror up to the industry. From there, the industry can identify whether:

- the secretariat has created a fair reflection of reality
- it likes what it sees.

The SRC is the first industry group to have an opportunity to comment on this paper. The Authority is likely to seek feedback from the Smart Grid Forum and the Critical Systems Security Information Exchange. Depending on all the feedback received, the Authority may also seek an international perspective.

# 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 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.

1.1.4 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.

## 1.2 The Authority Board requested that this paper be developed for the SRC's comment

1.2.1 At its 1 October 2014 strategic planning day, the Authority Board considered a broad range of topics, including information security. An action from that strategic planning day was for Authority staff to seek the advice of the SRC on the topic of information security.

## 1.3 Information security is broader than cybersecurity

1.3.1 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.

1.3.2 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]

[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

> "…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]

1.3.3 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

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.

## 1.4 Many aspects of information security are similar around the world

***There are a handful of different types of threat actors***

1.4.1 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.

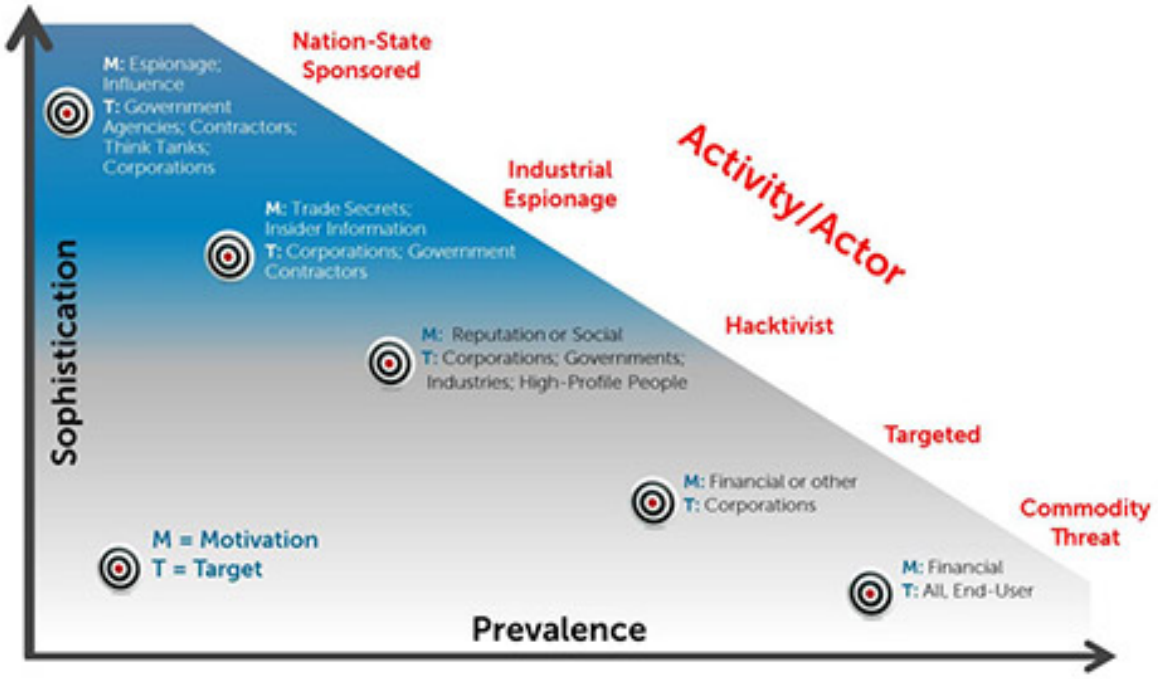
1.4.2 Information security breaches can also be self-inflicted without the help of any threat actor. In general, this would involve the active sending of important information to unintended recipients.

---

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

[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**

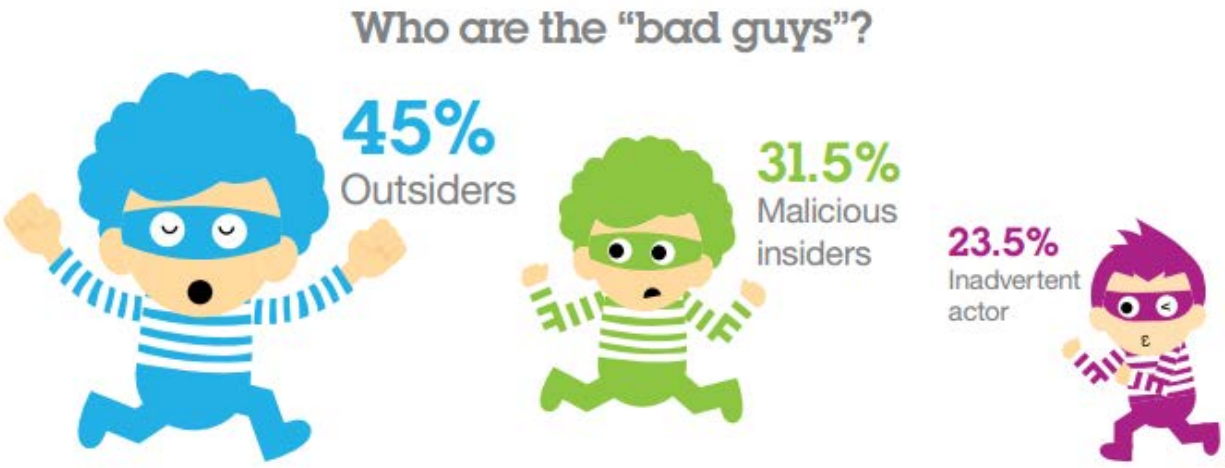



Source: Dell Secureworks[5]

***A substantial portion of intrusions involve insiders***

1.4.3 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**



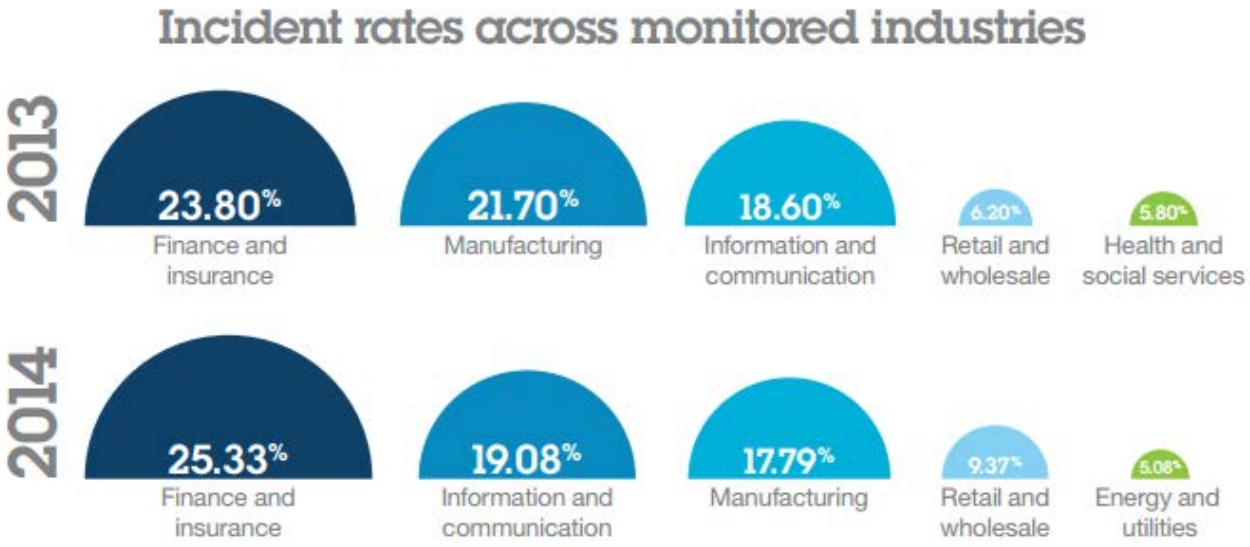

Source: IBM's 2015 Cyber Security Intelligence Index[6]

[5] From http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threat/understand-the-threat/

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

1.4.4 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 [7]

***The impact of information security breaches is sizable***

1.4.5 The annual global cost of cybercrime and cyberespionage has been estimated at over $400 billion (USD) by security firm McAfee in 2014.[8] No reliable direct estimates are available for New Zealand, but applying McAfee's estimated losses of 0.9% of New Zealand's gross domestic product indicates an annual cost of $2.1 billion (NZD).[9]

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

1.5.1 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 product of the United States and Israeli governments. Stuxnet reportedly destroyed about a fifth of Iran's nuclear centrifuges.[10]

---

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

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

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

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

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

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. [11]

c) 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.[12]

d) 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.[13]

[11] 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

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

[13] 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

# 2 New Zealand's electricity industry arrangements

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

2.1.1 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

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

g) transmission operator (Transpower).

2.1.2 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.

2.1.3 While information security is practiced at the level of the each individual organisation or person, these practitioners have very different incentives 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.

2.1.4 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.[14]

2.1.5 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.

2.1.6 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

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

protection. 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.

**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 (from a very high availability service with the registry to annual processing of the extended reserve manager) | Yes | No |
| Metering | Two (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 |

***Industry groups provide important information sharing***

2.1.7 The most important electricity industry group for information security in New Zealand is the Control Systems Security Information Exchange (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 2.2.2.

2.1.8 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 |

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

2.1.10 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

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

based on standards developed by the North American Electric Reliability Corporation (NERC), though they've been designed for application in New Zealand.

2.1.11 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.

2.1.12 The International Electricity Infrastructure Assurance Forum (IEIA) is an international public-private partnership open to participation from Australia, Canada, New Zealand 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.

## 2.2 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***

2.2.1 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)[17]

b) leading international engagement on cybersecurity

c) leading the ConnectSmart partnership that aims to "promote ways for individuals, businesses and schools to protect themselves online".[18]

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

2.2.2 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."[19]

2.2.3 As discussed in paragraphs 2.1.7-2.1.10, 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 More information from https://www.connectsmart.govt.nz/

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

2.2.4 NCSC issue various publications to assist organisations to improve their information security. One of these is an overview of information security for company directors. An extract from this overview is included as Appendix A.

2.2.5 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***

2.2.6 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.

2.2.7 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 *Interpretation 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."[20]

2.2.8 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.

2.2.9 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.

2.2.10 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.

2.2.11 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.

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

2.2.12 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

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

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

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

2.2.14 The members of the New Zealand Intelligence Community[21], 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.[22] 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 2.2.2, 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.[23]

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."[24]

2.2.15 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.

2.2.16 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 that "information…must be secure" and recommending that agencies *should* "follow applicable security guidelines". [25] In practice, unless a standard is not applicable or a better alternative is available, this means following:

---

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

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

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

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

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

a) the *Protective Security Requirements*

b) the NZISM.

2.2.17 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.

2.2.18 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 existing and role of the Privacy Commissioner, are set out in the Privacy Act 1993.

2.2.19 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."[26]

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

2.3.1 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.

2.3.2 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 key activities of the NZITF include training and information sharing.[27]

2.3.3 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.

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.[28]

b) The Orb provides a simple and safe way 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.[29]

2.3.4 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

---

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

[27] More information from http://www.nzitf.org.nz/

[28] More information from http://www.securitycentral.org.nz/

[29] More information from http://www.theorb.org.nz/

the New Zealand Security Information Forum (NZSIF). NZSIF seeks to promote expertise in information security among its membership and in the general community.[30]

2.3.5 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[31]

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[32]

d) has an award-winning expert (Dr Ryan Ko) leading its cybersecurity research and education.[33]

2.3.6 InternetNZ is a membership-based society that seeks to "promote the Internet's benefits and uses and protect its potential."[34] 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.

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

## 3.1 Information security best practice has a history of continual evolution

3.1.1 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.[35]

3.1.2 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.

3.1.3 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:

---

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

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

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

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

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

35 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)

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.

## 3.2 New Zealand may establish its own Computer Emergency Response Team

3.2.1 The NCPO have shown an interest in establishing a Computer Emergency Response Team (CERT) for New Zealand, similar to what other jurisdictions operate.[36]

3.2.2 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, having access to overseas experts could be valuable.

## 3.3 New Zealand could seek to establish an information security exercise or participate more in international exercises

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

a) Cyber Storm, a biennial exercise run by the United States Department of Homeland Security since 2006[37]

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

3.3.2 The CSSIE have previously considered running an information security exercise for New Zealand's energy sector. If the electricity industry participants are keen to participate, the Authority could assist another agency (such as the NCSC) to facilitate industry-wide involvement.

3.3.3 New Zealand organisations could aim to participate in a pre-existing exercise as an alternative to, or complementary to, a New Zealand-specific exercise.

[36] More information from http://www.dpmc.govt.nz/sites/all/files/publications/ncpo-speech-nzisf-11apr13.pdf

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

# 4 Next steps

## 4.1 The Smart Grid Forum and the CSSIE will have an opportunity to comment

4.1.1 The high-level description of the arrangements set out in section 2 of this paper will be circulated among members of the Smart Grid Forum and the CSSIE for comment. This should ensure the description is comprehensive and useful for any future steps.

## 4.2 International comparisons

4.2.1 The Authority will consider engaging relevant international experts to assess and compare the New Zealand electricity industry's information security arrangements against international benchmarks.

# 5 The SRC is being asked to consider whether the secretariat has accurately described the industry arrangements

5.1.1 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 consider that the paper provides a complete and accurate high-level description of the arrangements for information security in New Zealand's electricity industry? |
| **Q2.** | Does the SRC have any specific concerns about industry arrangements? (such as adequacy of incentives, gaps or duplication in responsibility, inter-organisational risks, inefficiencies, state sector arrangements, ability to cope with change) |
| **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? |

## Appendix A The NCSC's key questions for Boards

A.1.1 The NCSC has published a two-page overview of the sorts of questions Boards need to be asking of their organisations. An extract from this publication is repeated below as Figure 4.

A.1.2 These questions are focused at the organisational level rather than an industry-wide level. However, there may still be some value in SRC members considering these questions as a possible prompt for any insight into the electricity industry as an interconnected system or as a collective of individual organisations.

**Figure 4 - Key questions for Boards**

1. Does the Board understand what cyber security threats the organisation is vulnerable to?
2. Has the impact that a cyber security incident could have on your corporate reputation, share price, intellectual property and organisational wellbeing been identified? For example, what would the consequence be if sensitive information was lost or stolen?
3. Does the Board have a sufficient view of the business impact of cyber-security risks to the organisation?
4. Is there a plan to address cyber security risks?
5. Has the plan resulted in sufficient processes for the organisation to detect and respond to cyber incidents?
6. Does the Board have assurance that information assets are protected in a sustainable manner?
7. When failures occur, how resilient is the organisation and how would it recover?
8. Has the Board clearly communicated to the Executive its risk tolerance and expectations in relation to organisational cyber security?

Source: NCSC[38]

[38] Available from www.ncsc.govt.nz/resources

# 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 |