RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

POWER OF OPPORTUNITY

SESSION ID: PGR-F02

Cybersecurity in Singapore: Smart Nation, Safe Nation

Charmian Aw
Director, Drew & Napier LLC

Agenda

- Backdrop: the need for cybersecurity legislation in Singapore
- Legal framework
- Introduction to and applicability of the Cybersecurity Bill
- Key features of the Bill
- Potential areas for further clarification

RSA Conference 2017
Singapore

Backdrop: the need for cybersecurity legislation in Singapore

Notable cyber attacks in recent years

- Early 2014
  - Ministry of Foreign Affairs' IT system was breached.
- Mid 2014
  - 1,560 SingPass usernames and passwords, used by citizens to access Government services, were compromised.
- March 2016
  - 293 SingPass usernames and passwords were hacked by a Singaporean man and sold to a China syndicate.

Notable cyber attacks in recent years

- October 2016
  - Two cyberattacks disrupted a local telco provider's broadband service, resulting in the inability of the general public to access the internet for about two hours during each cyberattack.
- Early 2017
  - Attack against the internet access system of the Ministry of Defence (Mindef), resulting in the theft of personal data of approximately 850 national servicemen and Mindef employees.
- Mid 2017
  - Networks of two local universities were hacked in a bid to steal Government and research data.

How vulnerable is Singapore?

- Singapore ranks **5th** in terms of the **highest vulnerability economies to cyberattacks**
  - Deloitte Asia-Pacific Defence Outlook 2016
- The "Cyber Five" who are most heavily dependent on internet-based interactions (i.e., Singapore, South Korea, Australia, New Zealand, and Japan) **appears 9 times more vulnerable to cyberattacks than other Asian economies**.

Singapore's Smart Nation Cybersecurity Strategy

- Launch of the Singapore cybersecurity strategy in 2016 as part of Smart Nation Initiative
  - "*Singapore aspires to be a Smart Nation. But to be a Smart Nation, we must also be a safe, cyber nation. We must get cybersecurity right, to capture the benefits of a more connected world.*" -- Prime Minister Lee Hsien Loong
  - "*To realise these opportunities [that our Smart Nation can create], we must ensure our infrastructure is resilient and secure, protect personal data and information, and create a safe and conducive environment online*." -- Minister for Communications and Information, Dr Yaacob Ibrahim
  - 4 pillars of the strategy:
    - Building a resilient infrastructure
    - Creating a safer cyberspace
    - Developing a vibrant cybersecurity ecosystem
    - Strengthening international partnerships

RSA Conference 2017
Singapore

Legal Framework

Establishment of CSA

- **Establishment of the Cyber Security Agency (CSA) in 2015**
  - CSA is the central agency responsible for overseeing cybersecurity strategy, operation, education, outreach and ecosystem development.
  - It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information (MCI).
  - Current management in the CSA:
    - David Koh – Chief Executive and Commissioner
    - Teo Chin Hock – Deputy Chief Executive Development
    - Ng Hoo Ming – Deputy Chief Executive Operations

Legal Framework for Cybersecurity in Singapore

- Prior to the Cybersecurity Bill, there was no overarching cybersecurity legislation in Singapore.
- Instead, a patchwork of laws regulated cybersecurity.
- The **Computer Misuse and Cybersecurity Act** (Cap. 50A) was the primary legislation in Singapore dealing specifically with cybercrime.
- There were also other related laws such as:
  - Penal Code (Cap. 224)
  - **Personal Data Protection Act** 2012 (No. 26 of 2012)
  - **Sector-specific** regulatory/licensing requirements (e.g., MAS, IMDA)

RSA Conference 2017
Singapore

Introduction to and Applicability of the Cybersecurity Bill

Overview of Cybersecurity Bill

- Issued on 10 July 2017 by the MCI and the CSA.
- Public consultation to close on **3 August 2017**.
- Holistic approach to make Singapore resilient against increasingly sophisticated cyberattacks, raising preparedness and timely, effective responses when such attacks happen.
- Enforced by the Commissioner of Cybersecurity, deputy commissioners and assistant commissioners. Other authorised officers may also be appointed.

Key defined terms

- "Cybersecurity"
  - The security of a computer or computer system against unauthorised access or attack, to preserve the availability and integrity of the computer or computer system, or the confidentiality of information stored or processed therein.

Key defined terms

- "Computer"
  - An electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but does not include such other device as the Minister may, by notification in the Gazette, prescribe.
- "Computer system"
  - An **arrangement of interconnected computers** that is designed to perform one or more specific function, and includes —

    (a) an information technology (IT) system; and

    (b) an operational technology system such as an industrial control system (ICS), a programmable logic controller (PLC), a supervisory control and data acquisition (SCADA) system, or a distributed control system (DCS).

Key defined terms

- "Cybersecurity threat"
  - An act or activity on or through a computer or computer system, which is known or suspected, that **may imminently** jeopardise or adversely impact, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality, or integrity of information stored on, processed by, or transiting a computer or computer screen.
- "Cybersecurity incident"
  - An act or activity on or through a computer or computer system, that jeopardised or adversely impacted, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system.

RSA Conference 2017
Singapore

Key Features of the Cybersecurity Bill

Key Features

- 4 main regulatory areas:
  - Regulation of critical information infrastructure (CII)
  - Powers of the CSA to manage and respond to cybersecurity threats and incidents
  - Framework for sharing of cybersecurity information with and by CSA, and the protection of such information
  - Regulation and licensing of cybersecurity service providers

RSA Conference 2017
Singapore

(1) Regulation of CII

Regulation of CII

- What is “Critical Information Infrastructure”?
  - A computer or a computer system that is necessary for the continuous delivery of **essential services** which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

Regulation of CII

11 critical sectors have been identified as "essential services":

- Energy
  - Electricity generation, electricity transmission or electricity distribution services
  - Services for the supply or transmission of natural gas for electricity generation
- Healthcare
  - Emergency healthcare services
  - Hospital care services
  - Disease surveillance and response
- Functioning of the government
- Water
- Media
  - Services relating to broadcasting of free-to-air television and radio
  - Services relating to publication of newspapers
  - Security printing services

Regulation of CII

11 critical sectors have been identified as essential services:

- Info-communications
  - Fixed telephony services
  - Mobile telephony services
  - Broadband internet access services
  - Broadband internet access services
  - National domain name services.
- Security and emergency services
- Aviation
- Land transport
- Maritime
  - Monitoring and management of shipping traffic
  - Container terminal operations
  - General and bulk cargo terminal operations
  - Cruise and ferry terminal operations
  - Pilotage, towage and water supply
  - Bunker supply
  - Salvage operations
  - Passenger ferry operations

Regulation of CII

11 critical sectors have been identified as essential services:

- Banking and Finance
  - Retail and commercial banking services
  - Payments clearing and settlement services
  - Securities trading, clearing, settlement and depository services
  - Derivatives trading, clearing and settlement services
  - Monetary management operations and intervention operations services
  - Services related to mobilisation of official foreign reserves
  - Currency issuance
  - Services related to cash management and payments for the Government

Varying definitions of “essential services” in other jurisdictions

China

- Public communications and information service
- Energy
- Transport
- Water conservancy
- Finance
- Public services and e-government affairs
- as well as other CII that could cause serious damage to national security, the national economy and public interest if destroyed functionality is lost or data is leaked.

United States

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and agriculture
- Government facilities
- Health and public health
- Information technology
- Nuclear reactors
- Materials and waste transportation systems
- Water and wastewater systems

European Union

- Energy (i.e., Electricity, Oil, Gas)
- Transport (i.e., Air transport, Rail transport, Water transport, Road transport)
- Banking
- Financial market infrastructures
- Health sector
- Drinking water supply and distribution
- Digital infrastructure

Regulation of CII

- Who is an "owner of CII"?
  - A person who:
    - has **effective control** over the **operations** of the CII and has the **ability and right** to carry out **changes** to the CII; or
    - is **responsible** for **ensuring the continuous functioning** of the CII.
- CII may be owned either by the public or private sector.
- CII may be located wholly or partly in Singapore.

Regulation of CII

Obligations of owners of CII

- Provide information on the technical architecture of the CII
- Comply with codes and directions in relation to the CII
- *Inform* the Commissioner of any **intended change in ownership** of the CII no later than **90 days** *before* intended change
- Conduct **audits** and risk assessments for compliance with the Cybersecurity Bill once every **3 years**
- Inform the Commissioner of **material** changes made to the design, configuration, security or operation of the CII no later than **30 days**
- Furnish reports to the Commissioner
- Report cybersecurity incidents to the CSA
- Participate in cybersecurity exercises

RSA Conference 2017
Singapore

(2) Powers of the CSA – Response to Cybersecurity Threats and Incidents
(3) Sharing of Cybersecurity Information

Response to Cybersecurity Threats and Incidents

CSA officers will be empowered to conduct investigations, which will be exercised depending on the severity of the situation.

- **All** cybersecurity threats and incidents
  - Anyone relevant to the investigation may be examined to provide statements and relevant information
- **Serious** cybersecurity threats and incidents
  - The Commissioner has greater powers in such circumstances including:
    - Carrying out remedial measures
    - Entering premises with relevant computers and computer systems
    - Accessing such computers
    - Scanning computers for cybersecurity vulnerabilities
    - Seizing of computers of certain conditions are met
- **Emergency** measures and requirements
  - The Minister may (by issuing a certificate) authorise any person or organisation to take such measures or comply with such requirements to prevent, detect, counter any threat

Response to Cybersecurity Threats and Incidents

- A cybersecurity threat or incident is deemed **serious** if it meets any of the criteria below:
  - It creates a **real risk of significant harm** being caused to a CII.
  - It creates a **real risk of disruption** to the delivery of an essential service.
  - It creates a **real threat** to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.
  - The cybersecurity *threat* is **severe** based on harm that *may* be caused or the number of computers (CII or not) or information *at risk*.

Response to Cybersecurity Threats and Incidents

Failure to comply with the investigating officer/Minister's demands is an offence.

- **All** cybersecurity threats and incidents
  - A fine of up to S$5,000 and/or imprisonment up to 6 months
- **Serious** cybersecurity threats and incidents
  - A fine of up to S$25,000 and/or imprisonment up to 2 years
- **Emergency** measures and requirements
  - A fine of up to S$50,000 and/or imprisonment up to 10 years
  - Obstructing any person in complying with any measures as directed by the Minister is an offence and may be subject to a fine of up to S$50,000 and/or imprisonment of up to 10 years

Framework for Sharing of Cybersecurity Information

- To facilitate the investigation, an examined individual who discloses any information in **good faith** shall **not** be treated as being in **breach** of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.
- **Wilful** misstatement or refusal to provide information is an **offence**.

RSA Conference 2017

Singapore

Regulation of Cybersecurity Service Providers

Regulation of Cybersecurity Service Providers

- Introduction of a light-touch licensing framework.
- Currently, only CSPs that provide **penetration testing (*investigative*)** and **managed security operations centre monitoring (*non-investigative*) services** "for reward" require a licence.
- A practitioner's licence is also required for employees who provide investigative cybersecurity services.

Regulation of Cybersecurity Service Providers

- **Requirements** for licensed service providers include:
  - Qualifications and practical experience
  - The applicant (i.e. officer) is a fit and proper person
    - e.g., no criminal association, dishonesty, mental disorder, bankruptcy
  - The grant of licence is not against the public interest
  - Licence fees have been paid up
  - Such other requirements as may be prescribed

RSA Conference 2017
Singapore

Attribution of Offences

Attribution of Offences

- Query: When are individuals **personally liable** under the Bill?
- Attribution of offences can occur both ways:

  Between corporation ⇔ its officers / employees / agents

- "Officer": Any director, partner, member of management committee, chief executive, manager, secretary or other similar officer.

Attribution of Offences

- 1. An **officer's state of mind may be imputed to his/her corporation**:

  Where, in a proceeding for an offence under this Act, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that —

  (a) an officer, employee or agent of the corporation engaged in that conduct within the scope of his or her actual or apparent authority; and

  (b) the officer, employee or agent had that state of mind,

  is evidence that the corporation had that state of mind. (s 40(1)).

  - Applies to **limited** provisions only (a corporation's state of mind is not relevant for most offences):
    - S31(7)(a): where a person applying for a CSP licence makes any statement or furnishes any information that it knows is false or does not believe to be true.
    - S34(4): where a CSP knowingly makes a record that is false or misleading.
    - Disclosures in good faith to facilitate CSA investigations.

Attribution of Offences

- 2. Similarly, **offences by the organisation can be attributed back to its officers** (or individuals involved in its management and are in a position to influence its conduct), where such individuals:

  (i) *consented* or *connived*, or *conspired* with others, to effect the commission of the offence;

  (ii) is in any other way, whether by *act or omission*, knowingly concerned in, or is party to, the commission of the offence by the corporation; or

  (iii) knew or *ought reasonably to have known* that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence. (s 40(2)).

RSA Conference 2017
Singapore

Potential Areas for Further Clarification

Areas for Further Clarification

- "Owner of CII"
  - What is "effective control"?
    - e.g. Board, CEO, CTO, CRO, CISO, Head of Security and Security Administrators?
  - Who is "responsible for ensuring the continuous functioning" of the CII?
  - Can there be more than one owner?

Areas for Further Clarification

- Definition of “serious cybersecurity threats and incidents”
  - Meaning of “real risk”? Are hoaxes excluded?
  - Meaning of “threats”? Are insider threats included?
- Process of notifying in relation to incidents
  - Meaning of “significant” cybersecurity incidents?
  - Timing, form, content of notification?
- Notifying about “material” changes to design, configuration, security or operation of CII
  - Meaning of “material”? E.g. outsourced and product vendor changes?

Areas for Further Clarification

- Identification of licensable cybersecurity services
  - Currently applies to:
    - Suppliers of penetration testing and managed security operations centre monitoring services, for value; and
    - Employees providing investigative cybersecurity services.
  - Meaning of ‘for value’? (Consider intra-group arrangements)
  - Expansion of scope of licensable cybersecurity services?
- Licence application requirements
  - Licence fees?
  - Licence conditions?

To summarise… Impact of the Bill

- If you are an operator of essential services:
  - Your computers or computer systems may be designated as CII and there are obligations to be fulfilled.
- If you are a cybersecurity service provider:
  - You may have to be licensed.
- If you are a general member of the public:
  - Your assistance may be required for cybersecurity investigations.
- If you are a business dealing with CII or engaging a CSP:
  - You may need to consider contractual arrangements, and create new internal governance/reporting structures, cybersecurity incident management plans, and notification processes.

Submission of views/comments on the Bill

- All submissions should reach MCI/CSA no later than **5pm on 3 August 2017**
- Softcopy submissions only (Microsoft Word or PDF format)
- Submissions to be sent to csa_cs_bill_feedback@csa.gov.sg with the subject "Public Consultation for the Cybersecurity Bill"

RSA Conference 2017

Singapore

Thank You.