NEW SINGAPORE CYBERSECURITY BILL RELEASED FOR PUBLIC CONSULTATION

On 10 July 2017, the Ministry of Communications and Information (MCI) and the Cyber Security Agency of Singapore (CSA) released a proposed Cybersecurity Bill (Bill) for public consultation. The draft Bill aims to be a broad, omnibus cybersecurity law, instead of relying only on sector-specific legislation to govern cybersecurity. It demonstrates that cybersecurity continues to be a top priority for the Singapore Government.

Key issues

- The draft bill is intended as an overarching legislation to harmonise the requirements to protect critical information infrastructure (CII) across the public and private sectors in Singapore
- It seeks to impose duties on owners of CII, including that of reporting cybersecurity incidents
- Corporations in the banking, telecoms, transport, healthcare and energy sectors should be aware that they may be owners of CII and therefore subject to the cybersecurity requirements proposed under the bill

BACKGROUND

The CSA was set up by the Singapore Government in April 2015 as the central agency to oversee and coordinate all aspects of cybersecurity for the nation. The CSA has spent almost two years working on the Bill, which seeks to effectively address the increasingly sophisticated cyber threats to Singapore's national cyberspace.

The Bill has four objectives:

(a) to provide a framework for the regulation of critical information infrastructure (CII);

(b) to provide the CSA with powers to manage and respond to cybersecurity threats and incidents;

(c) to establish a framework for the mutual sharing of cybersecurity information with the CSA, and the protection of such information; and

(d) to establish a light-touch licensing framework for cybersecurity service providers.

COMMISSIONER OF CYBERSECURITY

The Bill proposes the appointment of a Commissioner of Cybersecurity (Commissioner) who will be responsible for the administration of the Bill (after it is passed). The Commissioner would also have other duties, including overseeing Singapore's cybersecurity.

CRITICAL INFORMATION INFRASTRUCTURE

A cornerstone of the proposed Bill is the protection of CII which is deemed to be necessary for the continuous delivery of Singapore's essential services. The security of CII was also referenced in the Singapore Cybersecurity strategy launched by the Singapore Prime Minister in October 2016.

In the Bill, CII is defined as a computer or a computer system that is necessary for the continuous delivery of "essential services". A list of "essential services" is included in the Bill and includes, amongst others, commercial banking services and payments clearing and settlement services, electricity generation services, water supply services, healthcare services and retail. New "essential services" may be designated by the Minister from time to time.

The Bill also allows the Commissioner to designate a computer or computer system as CII, thereby subjecting such computer or computer system to the regulatory regime in the Bill.

Who is a CII owner?

Under the Bill, an owner of CII (CII owner) is defined as a person who (i) has effective control over the operations of CII and has the ability and right to carry out changes to CII; or (ii) is responsible for ensuring the continuous functioning of CII.

A CII owner will receive a written notice from the Commissioner designating its computer or computer system as CII. CII owners who are aggrieved by the Commissioner's decision may, within 30 days of such designation, appeal against the designation to the Minister-in-charge of Cybersecurity (Minister), whose decision will be final.

Obligations of a CII owner

The Bill proposes that CII owners be subject to certain duties, including:

(a) a duty to appoint a contact person for the CII;

(b) a duty to report cybersecurity incidents in respect of the CII;

(c) a duty to conduct regular audits;

(d) a duty to conduct regular risk assessments of the CII;

(e) a duty to participate in cybersecurity exercises as required by the Commissioner;

(f) a duty to comply with such codes of practice or directions as issued by the Commissioner; and

(g) a duty to provide the Commissioner with information. This would include, for example, information on the technical infrastructure of the CII.

Essential Services relating to 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 Singapore Government

REGULATION OF CYBERSECURITY SERVICE PROVIDERS

Licensing of cybersecurity service providers

The Bill also seeks to introduce a light-touch licensing regime for cybersecurity service providers in Singapore. Two types of cybersecurity service licences are proposed: (i) Investigative Cybersecurity Service; and (ii) Non-Investigative Cybersecurity Service.

A licence for investigative cybersecurity services is required for cybersecurity services, which: (i) involve circumventing the controls implemented in another person's computer or computer system; or (ii) require the person performing the service to obtain a deep level of access to the computer or computer system in respect of which the service is being performed, or to test the cybersecurity defences of the computer or computer system. This includes penetration testing, and services to search for or exploit cybersecurity vulnerabilities in the computer or computer system of another person for the purpose of improving the cybersecurity of the computer or computer system.

A licence for non-investigative cybersecurity services is required for cybersecurity services which include managed security operations centre monitoring services, and services monitoring the cybersecurity of a computer or computer system of another person or assessing or monitoring the compliance of an organisation's cybersecurity policy.

In-house provision of cybersecurity services will be exempted from having to obtain a licence.

The Bill provides that providers of cybersecurity services who operate without a licence shall be guilty of an offence and may be liable to a fine of up to S$50,000 and/or imprisonment of a term of up to two years.

Requirements for licensed cybersecurity service providers

It is also proposed that licensed service providers (both investigative and non-investigative) be subject to requirements including:

(a) ensuring that key executive officers are fit and proper persons. The criteria for considering whether a person is fit and proper includes, amongst others, honesty, integrity and financial soundness;

(b) retaining service records for five years (e.g. client information, service provided, name of employee who provided the service);

(c) complying with a Code of Ethics (e.g. maintaining the confidentiality of client information); and

(d) implementing a process to ensure that employees performing the licensable services are fit and proper.

The CSA will conduct audits from time to time to ensure that licensing requirements are met. The Bill provides that a licensee who fails to comply with any licence condition shall be guilty of an offence and may be liable to a fine of up to S$10,000 and/or imprisonment of a term of up to one year.

The CSA will conduct further consultations with the industry before the licensing framework becomes operational.

POWERS TO INVESTIGATE CYBERSECURITY THREATS AND INCIDENTS

Under the Bill, the Commissioner and Minister will be given a range of powers which may be exercised depending on the severity of the situation. There are three proposed scenarios for the exercise of power:

All cybersecurity threats and incidents

Where the Commissioner has information regarding a cybersecurity threat or incident, the Commissioner may examine anyone relevant to the investigation, take statements and require the provision of relevant information.

A person so examined who, in good faith, discloses any information to an investigating officer 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.

Serious cybersecurity threats and incidents

Where the Commissioner receives information regarding a serious cybersecurity incident, the Commissioner may direct persons to carry out remedial measures and assist with the investigation, enter premises where relevant computers and computer systems are located, access such computers, and scan computers for cybersecurity vulnerabilities.

The Commissioner may also seize any computer or equipment for the purpose of carrying out further examination and analysis, if: (i) it is necessary for the investigation; (ii) there is no less disruptive way of achieving the investigation's purposes; and (iii) the Commissioner is of the view that the benefit from so doing outweighs the detriment caused to the owner of the computer system.

A cybersecurity threat or incident is deemed serious if: (i) it creates a real risk of significant harm being caused to CII; (ii) it creates a real risk of disruption being caused to the delivery of an essential service; (iii) it creates a real threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore; or (iv) the cybersecurity threat is of a severe nature, in terms of the severity of harm that may be caused or the number of computers or value of information put at risk, whether or not the computers or computer systems put at risk are of the nature of CII.

Emergency measures and requirements

The Minister may authorise any person or organisation to take such measures or comply with such requirements as may be necessary to prevent and detect, or counter any threat to a computer or computer service or any class of computers or computer services.

To do so, the Minister must be satisfied that such measures are necessary to prevent, detect or counter any threat to the essential services or national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

CONCLUSION

The Bill demonstrates the Singapore Government's commitment to national cybersecurity. It will apply to any CII located wholly or partly in Singapore.

As an indication of the seriousness with which cybersecurity is viewed, the Bill proposes that officers of a body corporate may also be liable, if the offence which the body corporate is guilty of, was committed with: (i) the consent or connivance of the officer; or (ii) attributable to any neglect on the officer's part.

The MCI and CSA have invited all industry members and members of the public to comment on the draft Bill by 3 August 2017. We will be preparing a response, and invite comments for inclusion in (or expansion upon) our response.

CLIFFORD
CHANCE

CONTACTS

Nish Shetty
Partner

T +65 6410 2285
E nish.shetty
@cliffordchance.com

Lena Ng
Partner

T +65 6410 2215
E lena.ng
@cliffordchance.com

Kabir Singh
Partner

T +65 6410 2215
E kabir.singh
@cliffordchance.com

Paul Landless
Partner

T +65 6410 2235
E paul.landless
@cliffordchance.com

Chui Lijun
Senior Associate

T +65 6506 2752
E lijun.chui
@cliffordchance.com

Ho Wan Yi
Associate

T +65 6410 2275
E wanyi.ho
@cliffordchance.com

www.cliffordchance.com
www.cavenaghlaw.com.sg

Clifford Chance Asia

12 Marina Boulevard, 25th Floor Tower 3, Marina Bay Financial Centre, Singapore 018982

Clifford Chance Asia is a Formal Law Alliance between Clifford Chance Pte Ltd and Cavenagh Law LLP.

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • Jakarta* • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

*Linda Widyati & Partners in association with Clifford Chance.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.