NATIONAL UNIVERSITY OF SINGAPORE

IFS 4101 – LEGAL ASPECTS OF INFORMATION SECURITY

AY2021/2022, Semester 2, Week 13

CYBERSECURITY LAWS

I. INTRODUCTION

You have learned that laws can be categorised in many ways. There is another way to categorise laws, that is to describe them as proscriptive, interpretive or prescriptive. Proscriptive laws are those that dictate what must not be done. Criminal laws fall comfortably into this category of laws. Interpretive laws set out the framework for interpreting certain types of situations. The Evidence Act and the Interpretation Act fall into this category.

The last category is called prescriptive laws. These are laws that mandate certain types of behaviour to be carried out actively. You have seen some of this in the Personal Data Protection Act, which requires those subject to the act to conduct reasonable assessments and implement reasonable safeguards to protect data. The Cybersecurity Act 2018 ("CSA") also fall into this category of laws as it establishes a licensing regime for certain activities that, absent the licensing activity, could constitute a crime under the Computer Misuse Act (e.g., penetration testing) and it also requires those who manage critical information infrastructure ("CII") to actively engage in reporting of security incidents and conducting annual security assessments.

Prescriptive laws tend to be rare in common law jurisdictions because of the philosophical underpinning of the common law judicial system. The common law system operates in a more *laissez-faire* manner, believing that citizens should be left alone with limited interference activities and the law stepping in only when corrective actions need to be taken. Civil law jurisdictions, such as those in China, Japan, Korea, Thailand, Continental Europe and the former colonies of countries with a civil law tradition, tend to impose prescriptive requirements on their citizens at a higher frequency. You see this in the cultural reaction to the mask mandates imposed over Covid-19 – common law countries such as the US, UK and India had much greater difficulty creating legislation to mandate masks, whereas civil law jurisdictions such as the China, Germany and Italy could get the mask mandate laws enacted much faster.

Why does it make sense to enact prescriptive laws? When there is a recognition that the lack of regulation will lead to a "tragedy of the commons." This term, coined by the evolutionary biologist Garrett Hardin in 1968, describes how rational choices made by individuals to do good – reaching the goal of economic success – ends up allowing those with less social conscience to create the tragedy. In the world of cyberspace, allowing individuals and companies the freedom to maximise profit by implementing the cheapest technical safeguards (or no safeguards) to protect data could wreak havoc on society, causing the breakdown of essential services and the destruction of lives.

Recognizing this to be the case, the Singapore Parliament adopted the CSA in 2018. Indeed, the Minister for Communications and Information (Assoc Prof Dr Yaacob Ibrahim) recognized in his opening remarks during the Second Reading of the Cybersecurity Bill, that "[p] rotection against cyber-attacks needs to start with organisations and individuals

taking responsibility for the cybersecurity of their own computer systems." (*Emphasis added*.)

You should read the legislative history behind the Cybersecurity Bill to understand Singapore's philosophy towards cybersecurity threats. The following three readings will give you some idea about Singapore's view towards cybersecurity threats:

- Second Reading, Cybersecurity Bill 2018, Official reports – Parliamentary Debates (Hansard), Feb. 5, 2018.
- Public Consultation Paper on the Draft Cybersecurity Bill (10 Jul 2017) [LINK]
- Report on Public Consultation on the Draft Cybersecurity Bill (13 Nov 2017) [LINK]

II. Key Terms

To understand the CSA, you need to understand the following defined terms (see Section 2 of the CSA):

- critical information infrastructure
- essential service
- cybersecurity incident
- cybersecurity

As you review these key terms, answer these questions:

1. What is not an essential service? Name a few examples.

2. Is the term "cybersecurity" well-defined based on your understanding from a technical standpoint? How is sub-clause (b) in the definition of the term "cybersecurity" different from sub-clause (c)?

III. Scope of CSA

The scope of the CSA is detailed in Section 3. Notice to whom the CSA applies.

IV. Critical Information Infrastructure Provider

A. Designation as CII

How does something qualify as a critical information infrastructure ("CII")? Read Section 7 of the CSA. What can you do if you dispute the designation of your company's infrastructure as CII? Why would you want or not want to be classified as CII?

B. Investigating the Designation as CII

Read Section 8 of the CSA. As the CIO, would you be concerned about this clause? How does this clause affect the operations of any company that operates a computer or computer system? What type of documentation do you have to create to get yourself ready to respond to a Commissioner request?

C. Information Disclosure Obligation

If you are the CIO of a company that owns CII, what do you need to get ready at all times? Read Section 10 of the CSA. What do you need to do to be ready to comply with Section 10 at all times?

D. Compliance with Codes, Standards and Written Directions

Read Sections 11 and 12 of the CSA. How would these sections affect how a CIO plans her work and makes her decisions should she be working for a company that owns CII?

E. Reporting Obligations

Read Sections 13 and 14 of the CSA to understand the reporting requirements. In particular, in the case of an incident, when must you report to the Commissioner? Review Section 2 to make sure that you are interpreting the defined terms correctly before you answer this question.

F. Other Obligations

Read Sections 15 and 16 of the CSA.

Questions

1. What are the duties of a CII owner under the CSA?
2. Can an owner of CII choose not to follow/comply with any of these obligations?

V. Responding to Cybersecurity Threats and Incidents

A. Normal Cybersecurity Incidents

Read Section 19 of the CSA.

Questions

1. How should a company respond to a **normal** cybersecurity incident?
2. What information/assistance should it provide?
3. What information/assistance is it entitled to not provide?

B. Serious Cybersecurity Incidents

Read Section 20 of the CSA.

Questions

1. How should a company respond to a **serious** cybersecurity incident?
2. What information/assistance should it provide?
3. What information/assistance is it entitled to not provide?

C. Emergency Cybersecurity Incidents

Read Section 23 of the CSA.

Questions

1. How should a company respond to an **emergency** cybersecurity incident?

2. What information/assistance should it provide?

3. What information/assistance is it entitled to not provide?

VI. Licensing Cybersecurity Service Providers

A. What is a Cybersecurity Service?

Review Section 2 of the CSA.

Question

1. What constitutes cybersecurity service?

2. What does not?

B. Licensable Cybersecurity Services

Review the Second Schedule of the CSA.

Questions

1. Can a company conduct the activities described in the Second Schedule for its affiliated company?

2. Must it obtain a license to do so?

C. Conditions of License

Review Sections 24, 26, 27, 29-32 of the CSA.

Questions

1. Why do you think the CSA needs to include these sections?

2. How do these sections impact you personally, if you wish to become a CIO at Singtel one day?

VII. Evaluating the Cybersecurity Act 2018

What should you do to best prepare your company for the CSA?

In particular, consider: the duties of your company, its immunities under the Cybersecurity Act, its costs of compliance, and dealings with the breadth of the CSA Commissioner's powers.