LEGAL ASPECTS OF INFORMATION SECURITY IFS4101

WEEK 13, WELLY TANTONO, DIS, SOC, NUS

FINDING THE RIGHT SOLUTIONS TO PERSONAL DATA MANAGEMENT

1. In each of the following scenarios, which scheme or schemes (i.e., legal, technical or operational safeguards) would you recommend to an organisation to ensure that it remains compliant to the PDPA's requirements that personal data be kept accurate and complete; remains protected from unauthorised access; and is no longer retained when the purposes for which it was collected is no longer necessary ? (Be prepared to discuss the details of each solution that you propose.)

- inadequately documented personal data (source, nature of data, purpose, currency, etc. are all inadequately documented)
- poor (physical and electronic) document management
- unmonitored outgoing business email communications
- weak or non-existent information security implementations for hardware
- use of in-house or third party software tools for managing personal data
- social engineering attacks

2. What were the factors that you considered in selecting the scheme that you propose to use to address the problems above?

INVESTIGATING AND REPORTING CYBERSECURITY INCIDENTS – CYBERSECURITY ACT 2018

CYBERSECURITY

- Cybersecurity is the art of protecting networks, devices, and data from **unauthorized access** or **criminal use** and the practice of ensuring **confidentiality, integrity, and availability** of information. - *Definition given by CISA*
- Definition in Section 2 of the Cybersecurity Act 2018:
  - "Cybersecurity" means the state in which a computer or computer system is **protected** from unauthorised access or attack, and because of that state —
    a. the computer or computer system continues to be available and operational;
    b. the **integrity** of the **computer or computer system** is maintained; and
    c. the **integrity** and **confidentiality** of **information stored in, processed by or transmitted** through the computer or computer system is maintained;

WHY IS CYBERSECURITY IMPORTANT?

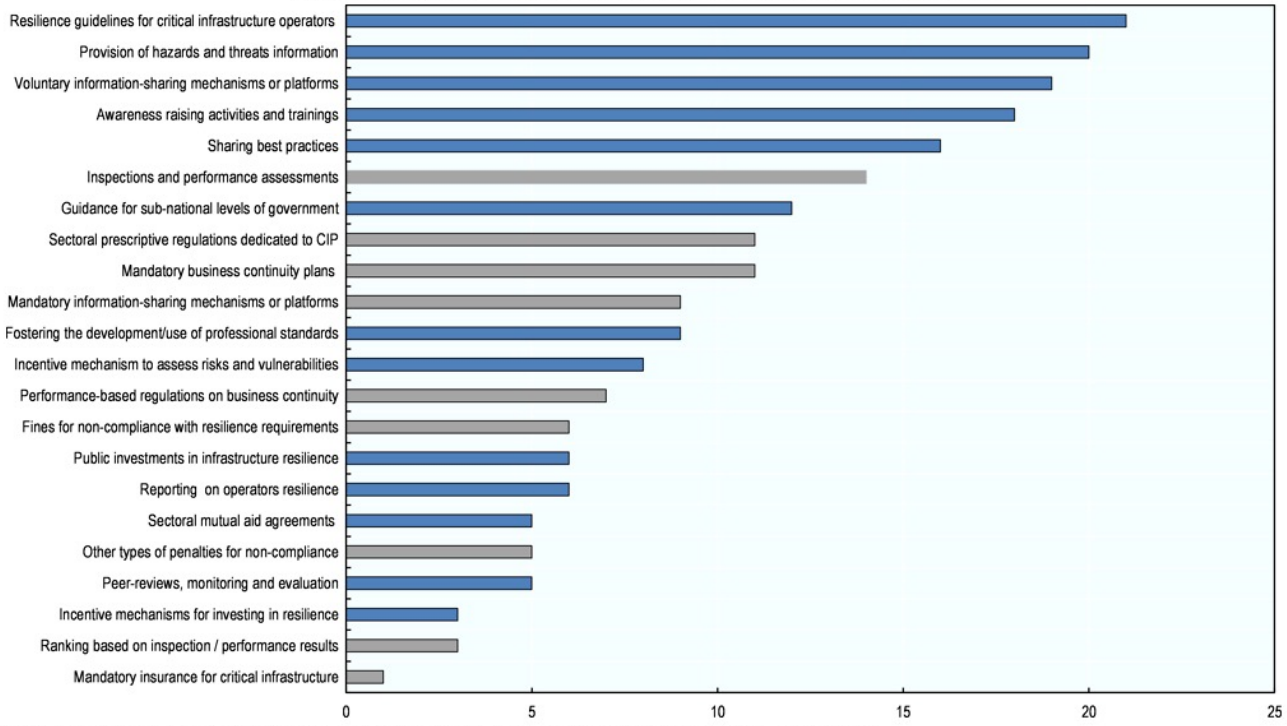
- Increasing digitalization
- General population's poor understanding of how the cyberworld works (modalities problem)
- Industrial Revolution 4.0 / Smart Nation
- Nature of digital
  - Digital = scale (i.e., we concentrate effort on developing that one thing that runs repetitive processes very cheaply)
  - Concentrates risks on single points of failure = single points of attack from the perspective of attackers
  - Single points of attack increases the rewards / returns for those who investigate their resources into studying that single weakness, which, in turn, incentivizes more actors to concentrate on attacking concentrations of weaknesses.

SINGAPORE'S REGULATORY PHILOSOPHY TOWARDS CYBERSECURITY

- Recognition that cyberattacks are increasing in frequency, sophistication **and impact**
- Sophistication of actors – no longer about the badly socialised teenagers who lurk in IRC, but increasingly, industrial espionage and national security espionage by state actors
- Digitalisation of essential services means impact of a failure of security of critical information infrastructure affects the entire society
  - E.g., UK NHS not be able to provide essential hospital services because of WannaCry ransomware – how many people died because the system could not handle the scheduling / communications of emergencies?
  - E.g., Colonial Pipeline ransomware
- Singapore especially vulnerable because of its economic strategy – to be at the cross-roads of trade means to be at the crossroads of communication. This requires fast adoption of new communication technologies => digitalisation => high risk

CYBERSECURITY POSSIBLE POLICY RESPONSES

Figure 3.3. **Policy tools for critical infrastructure resilience across OECD countries**

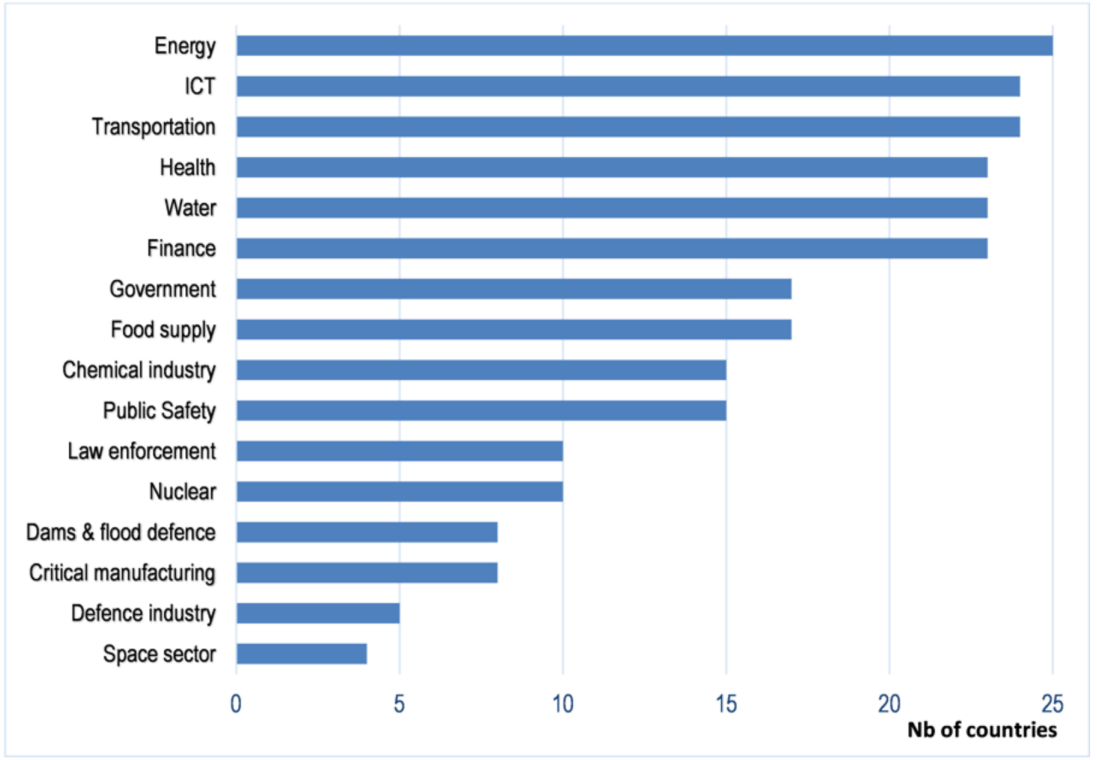


Note: 22 OECD countries responded to the survey as of 10 September 2018 – mandatory tools are in grey, voluntary tools are in blue.

Source: OECD Survey on Critical Infrastructure Resilience (2018)

SAFEGUARDING AGAINST CYBER ATTACKS ON CRITICAL INFRASTRUCTURE

Figure 3.1. **Sectors of designated critical infrastructure across OECD countries**



Note: Answers received from 25 OECD countries.

Source: OECD Survey on Critical Infrastructure Resilience and Security (2018)

IS THERE A NEED FOR A NEW PIECE OF LEGISLATION?

- Computer Misuse (Amendment) Act (Act 25, of 2003) provides for the following:

15A. – (1) Where the Minister is satisfied that it is necessary for the purposes of preventing or countering any threat to the national security, essential services, defence or foreign relations of Singapore, the Minister may, by a certificate under his hand, authorise any person or organisation specified in the certificate to take such measures as may be necessary to prevent or counter any threat to a computer or computer service or any class of computers or computer services.

(2) The measures referred to in subsection (1) may include, without limitation, the exercise by the authorised person or organisation of the powers referred to in section 15.

(5) In subsection (1), "essential services" means —

(a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation or public key infrastructure; and

(b) emergency services such as police, civil defence or medical services.

WHAT IS SECTION 15A MEANT TO COVER?

- In the Explanatory Statement of the Computer Misuse (Amendment) Bill 2003:

"*Clause 3 inserts a new section 15A to allow necessary measures to be taken, with the authorisation of the Minister, for the purposes of preventing or countering any threat to a computer or computer service or any class of computers or computer services. Such measures may be taken by an authorised person or organisation if the Minister certifies that he is satisfied that such measures are necessary for the purposes of preventing or countering any threat to the national security, essential services, defence or foreign relations of Singapore.*"

Not confined to threats against national security: threats against essential services count as threats against "national security" – concept of Critical Information Infrastructure

Not confined to existing threats, but encompasses potential/future threats

Very broad, extensive measures might be taken - scope of "such measures as may be necessary to prevent or counter any threat to a computer or computer service or any class of computers or computer services"

SECTION 15A WAS MEANT TO DEAL WITH EXTRAORDINARY CYBERATTACKS

"However, the CMCA, which mainly deals with cybercrimes such as the unauthorised access of computer material, does not provide a regulatory framework for the **routine and proactive** protection of CII."

- Minister Dr. Yaacob Ibrahim, *Second Reading of CSA*, 5 Feb 2018

CYBERSECURITY ACT

New framework to:

- strengthen protection of CII against cyberattacks
  - CII owners have duties to protect CIIs under their responsibility, **even before** a cybersecurity incident has occurred
  - sector coordinators to raise level of cybersecurity within sector
- authorise Cyber Security Agency of Singapore (CSA)
  - receive and share cybersecurity information with relevant parties to prevent, detect, counter, investigate any cybersecurity threat or incident (based on s 15A, CMCA)
- licensing framework for selected cybersecurity service providers
  - penetration testing and managed security operations centre services
  - to provide greater assurance of safety and security, address information asymmetry and improve standards

MCI and CSA, 10 Jul 2017

LEGISLATIVE DEVELOPMENT

- MCI/CSA opened up proposed Cybersecurity Bill for public consultations in July 2017
- Public consultations
  - 92 submissions received
  - respondents ranged from Amazon Web Services to DLA Piper, from KPMG to M1, from NTU to Singtel, from SP Group to Zurich Insurance, from Association of Banks to American Chamber of Commerce
  - generally supportive of legislative framework to protect CIIs and sharing of cybersecurity information
  - expressed reservations as to proposed (mandatory) licensing framework

LEGISLATIVE CONCESSIONS

- MCI / CSA revised Bill in 3 main ways
  - narrower definition of CII and only for CII that is designated as such. Computer systems in supply chain supporting CII operations will not be designated as CIIs

  >> What does this mean in light of SingHeath, Solar Winds and Microsoft? Vulnerabilities appear to reside in suppliers!

  - duties of CII owners to be made consistent with **sector specific codes of practices and standards**
  - distinction between investigative and non-investigative licensable services removed; only penetration testing and managed security operations centres will be licensed
- Cybersecurity Bill was signed into law by President on 2 March 2018 and came into operation on 31 August 2018.

11 SECTORS ARE CONSIDERED ESSENTIAL SERVICE

- 11 industries and sectors (see the First Schedule of the CSA)
  - Energy
  - Info-communications
  - Water
  - Healthcare
  - Banking and Finance
  - Security and Emergency Services
  - Aviation
  - Land Transport
  - Maritime
  - Government
  - Media
- What is *not* an essential service?

Food is not here, as compared to the OCED

CYBERSECURITY ACT – KEY DEFINITIONS

- Critical information infrastructure – CII
  - a computer or a computer system in respect of which a designation under section 7(1) is in effect
  - if no designation is in effect, computer/system is NOT CII
- Cybersecurity incident
  - an act or activity carried out without lawful authority on or through a computer/system that **jeopardises** or **adversely affects** its cybersecurity **or** the cybersecurity of **another computer/system**

SCOPE OF CSA: SECTION 3

To whom or what does the CSA apply?

- Part 3 (except Section 8) applies to any CII
- Section 8 applies to any computer/system
- Computer/computer system located **wholly or partly in Singapore**
- CSA applies to the Government
  - But Government not liable to prosecution
- No immunity from prosecution for public officers or Government contractors

DESIGNATING SOMETHING AS CII – SECTION 7

- Definition
  - computer/system is necessary for continuous delivery of an "essential service"
  - loss/compromise will have debilitating effect on availability of essential service in Singapore
  - computer/system is located wholly/partly in Singapore
- "essential service"
  - any service essential to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, and specified in the First Schedule

DESIGNATING SOMETHING AS CII – SECTION 7

- written notice
  - Identify computer/system
  - Identify owner
  - Inform owner of duties/responsibilities
  - Provide name/contact of officer assigned by CSA Commissioner
  - Inform owner of rights of representation against designation and right/procedure of appeal
- designation valid for 5 years unless withdrawn by Commissioner
- putative "owner" may "redirect: notice to person with effective control over operations of computer/computer system and ability and right to carry out changes
- Commissioner to be informed if owner ceases to have control over operations, loss of ability *and* right to carry out changes
- Perm Sec treated as owner of CII owned/operated by Ministry
- possible Appeal to Minister: s 17(1)(a)

INVESTIGATION OF DESIGNATION AS CII – SECTION 8

- Commissioner may give notice to any person who "appears to be exercising control" over computer/system to provide "such relevant information" relating to computer/system for "purpose of ascertaining" whether computer/system is CII
  - information to include, about computer/system: function; person(s) served; design; such other information as Commissioner may require
  - failure to comply "without reasonable excuse" is an offence: s 8(4), except for information subject to right, privilege, immunity, obligation, limitation in law, contract, rules of conduct: s 8(5)

alot of good paper work needs to be in place as there is alot of justification on why certain designs are like that

ADDITIONAL INFORMATION REQUEST – SECTION 10

Commissioner may give notice to CII owner to provide information about:

- CII's design, configuration and security
- design, configuration and security of any "other computer/system" under owner's control interconnected to/communicates with CII
- CII's/any "other computer/system's" operation
- such other information as Commissioner may require to ascertain level of cybersecurity of CII
- failure to comply "without reasonable excuse" is an offence: s 10(2), except for information subject to right, privilege, immunity, obligation, limitation in law, contract, rules of conduct: s 10(3)
- disclosure in breach of contract is "not treated as being in breach of any contractual obligation" if done in good faith and for complying with notice: s 10(4)
- Commissioner to be informed if "material change": s 10(5), (6); failure to inform "without reasonable excuse" is an offence: s 10(7)

COMMISSIONER'S ORDERS: GENERAL & SPECIFIC

- publication of codes of practice/standards of performance: s 11
  - no legislative effect: s 11(5), but every CII owner has to comply: s 11(6)
  - waivers possible: s 11(7)
  - possible Appeal to Minister: s 17(1)(c)
- written directions by Commissioner: s 12
  - direction to require action to be taken by owner in relation to cybersecurity threat; compliance with codes of practice/standards; appointment of auditor to audit owner; "such other matters" as Commissioner may consider necessary/expedient
  - notice recipient to be given notice, recipient may make representations/objections
  - failure to comply "without reasonable excuse" is an offence: s 12(6)
  - possible Appeal to Minister: s 17(1)(b)

DUTIES OF THE CII OWNER

- report change in CII ownership (by relevant person): s 13
  - failure to comply "without reasonable excuse" is an offence: s 13(2)
- report cybersecurity incident in respect of CII: s 14
  - for prescribed cybersecurity incident in respect of CII
  - for prescribed cybersecurity incident for computer/system interconnected/communicates with CII
  - any other type of cybersecurity incident in respect of CII specified by Commissioner
  - "owner of a CII must establish such mechanisms and processes" for "detecting [~~prescribed~~] cybersecurity threats and incidents" as set out in code of practice: s 14(2)
  - failure to report "without reasonable excuse" is an offence: s 13(3)
  - "There is no obligation for a CII owner to report a cybersecurity incident in respect of other infrastructure that it owns, **where such infrastructure is not connected to the CII**." *Minister Yaacob, 5 Feb. 2018*

DUTIES OF THE CII OWNER

- audit CII for compliance with CSA, codes and standards (at least) once every 2 years: s 15(1)(a)
- conduct cybersecurity risk assessment of CII (at least) once every year: s 15(1)(b)
- provide report of audit/assessment to Commissioner: s 15(2); failure to report "without reasonable excuse" is an offence: s 15(8)
- participate in cybersecurity exercise to "test state of readiness ... [to respond] to significant cybersecurity incidents": s 16(2)
  - possible Appeal to Minister: s 17(1)(b)
- Commissioner may order:
  - s 15(1)(a) reaudit if unsatisfactory: s 15(3)
  - s 15(1)(b) reassessment if carried out unsatisfactorily, or carry out further steps for evaluation (at owner's cost): s 15(5)
  - s 15(4) audit for non-compliance with code/standard, or if information is false, misleading, inaccurate or incomplete (at owner's cost)
  - s 15(1) reaudit/reassessment if Commissioner notified via s 10(5) of material change to design, etc. of CII, or Commissioner otherwise becomes aware of such material change

here are some of the expensive pre-emptive costs that CII must have

EVALUATING THE DUTIES OF CII OWNER

- CII classification may make or break a company
  - breadth of CII classification in First Schedule
  - onerous business obligations imposed
  - business must be prepared to challenge designation, if CII operations are incidental
  - "necessary", "continuous delivery", "essential service", "debilitating effect", "wholly/partly in Singapore"
  - CSA's clarification: "computer systems in the supply chain supporting the operation of a CII will not be designated as CII" *cf.* s 14(1)(b)
- costs of pre-emptive architectural development, detection mechanism and process and compliance: s 14(2); costs borne by company
- duty extends not just to CII infrastructure but non-CII infrastructure connected to CII infrastructure: s 14(1)(b)
- duty to report cybersecurity breaches to CSA vs duty to other regulators vs duty to clients, customers

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #1

Where information has been received, Commissioner may exercise powers (as are necessary) to investigate cybersecurity threat or incident: s 19

- purpose: assess (potential) impact of threat/incident; prevent any/further harm; prevent further incident: s 19(1)
- require any person to attend at time/place to answer any question or provided signed written statement about threat/incident: s 19(2)(a)
  - failure to comply will trigger Magistrate's order to attend before Commissioner: s 19(5)
- require any person to produce any record/document/copy or provide any information, which incident response officer considers to be related to any matter relevant to investigation, at specified time/place and manner/form : s 19(2)(b), (3)
- inspect, copy, take extracts of record/document/copy, for free: s 19(2)(c)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #1

- examine orally any person who appears acquainted with threat/incident, and reduce person's statement to writing: s 19(2)(d), (4)
- failure to comply "without reasonable excuse" or wilfully misstates is an offence: s 19(8), except for information subject to right, privilege, immunity, obligation, limitation in law, rules of conduct, but not contract: s 19(6),
- any examination/compliance in contractual breach but done with reasonable care and in good faith is "not treated as being in breach of any contractual obligation": s 19(7)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #2

Where information has been received that satisfies the "severity threshold", Commissioner may exercise powers (as are necessary) to investigate cybersecurity threat or incident: s 20

- "severity threshold": risk of significant harm being caused, or risk of disruption to, CII; threat to national security, defence, foreign relations, economy, public health, public safety, public order; 'severe nature': severity of harm or number of computers or value of information put at risk, whether or not computers/systems are CII: s 20(3)
- require any person to attend at time/place to answer any question or provided signed written statement about threat/incident: s 20(2)(a)
  - failure to comply will trigger Magistrate's order to attend before Commissioner: s 19(5)
- require any person to produce any record/document/copy or provide any information, which incident response officer considers to be related to any matter relevant to investigation, at specified time/place and manner/form : s 20(2)(a)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #2

- inspect, copy, take extracts of record/document/copy, for free: s 20(2)(a)
- examine orally any person who appears acquainted with threat/incident, and reduce person's statement to writing: s 20(2)(a)
- direct <u>any person</u> to carry out such remedial measures, or cease carrying on such activities – e.g., remove malicious software, install software updates, temporary disconnection, redirection of traffic - in relation to computer/system that officer has reasonable cause to suspect is/was affected by incident, to minimize cybersecurity vulnerabilities in computer/system: s 20(2)(b)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #2

- require computer/system owner to "take any action" to assist in investigation – e.g., preserve state of computer/system by not using it, monitoring; performing vulnerability scan and assess manner/extent affected; allow officer to connect any equipment to computer/system, or install any program as is necessary: s 20(2)(c)
- enter premises of affected computer/system, after giving notice to owner/occupier: s 20(2)(d)
- assess, inspect, check computer/system suspected of being affected by incident, or search any data in/available in such computer/system: s 20(2)(e), and get assistance from any person who is user, in charge or operator to gain such access: s 20(4)
- scan computer/system to detect cybersecurity vulnerabilities: s 20(2)(f)
- take copy/extracts of any electronic record/program suspected was affected by incident: s 20(2)(g)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #2

- with consent of owner, take possession of any computer/equipment for further examination/analysis: s 20(2)(h)
  - may take without owner's consent if necessary, no less disruptive method to achieve purpose, and benefit outweighs detriment to owner: s 20(5), but must return immediately after completion: s 20(6)
- failure to give any information, statement or produce any record "without reasonable excuse" or wilfully misstates is an offence: s 20(7)(a~~), except for information subject to right, privilege, immunity, obligation, limitation in law, rules of conduct, but not contract: s 19(6)~~; failure "without reasonable excuse" to comply with Magistrate's order is an offence: s 20(7)(b); failure "without reasonable excuse" to comply with lawful demand under s 20 is an offence: s 20(7)(d)

all information must be given to the Commissioner unlike in the lower severity threshold

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #3

Where necessary for preventing, detecting, countering any serious and imminent threat to essential service, national security, defence, foreign relations, economy, public health, public safety, public order, Minister may (re-enactment of s 15A, CMCA):

- authorise or direct any person/organisation in certificate to "take such measures or comply with such requirements as may be necessary to prevent, detect, counter any threat to a (or any class of) computer/system: s 23(1)
- exercise any powers under CPC, ss 39(1)(a), (b), (2)(a), (b) [power to access computer to conduct police investigations into arrestable offence], 40(2)(a)-(c)
- [power to access decryption information]: s 23(2)(a)
- require any person to provide any information – including design, configuration, operation, cybersecurity of any computer, program, system necessary to identify, detect, counter such threat: s 23(2)(b)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #3

- be provided any information (including real-time information) from any computer controlled/operated by specified person, or obtained by specified person from another person pursuant to s 23(2)(b): s 23(2)(c)
- be provided report of breach/attempted breach of cybersecurity viz s 23(1) report: s 23(2)(d)
- failure to take any measure or comply with any requirement "without reasonable excuse" is an offence: s 23(4), except for information subject to legal privilege (but not right, immunity, other privilege, contract, rules of professional conduct: s 23(3))
- obstruction "without reasonable excuse" of person taking any s 23(1) measure, or failure to comply with any direction "without reasonable excuse" is an offence: s 23(5)
- no civil or criminal liability incurred by a specified person (and a person directed by a specified person) for doing/omitting to do any act done in good faith and for purpose of/taking any measure/compliance with s 23(1) measure: s 23(6)
- no breach of legal, contractual, professional restriction against disclosure of information by specified person (and person who discloses information to specified person) in compliance with s 23(1) measure: s 23(7)

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS #3

- specified person (and person to whom specified person provides information) under s 23(1) must not use or disclose information, except with written permission of originator/third person, or to prevent/detect/counter threat, or to police officer/law enforcement any information which discloses the commission of any offence, or pursuant to court order/legal requirement: s 23(8); otherwise offence: s 23(9)
- if an offence is disclosed under s 23, no information for that offence may be admitted in evidence, and no witness is obliged to disclose particulars of any informer, or answer any question that would lead to discovery of informer: s 23(10), and any information in any evidence which names or describes or may lead to informer's discovery must be concealed: s 23(11)
- cf. s 45 (protection of informers who provide info that may lead to CII prosecution

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS (SUMMARY)

	General Cybersecurity Threat (s.19)	Severe Cybersecurity Threat (s.20)	Critical Cybersecurity Threat (s.23)
Object	• Assess (potential) impact of threat/incident • Prevent any/further harm • Prevent further incident	• Risk of significant harm being caused, or risk of disruption to, CII or provision of "essential service" • Threat to national security, defence, foreign relations, economy, public health, public safety, public order • Threat satisfies "severity" threshold	Serious and imminent threat to essential service, national security, defence, foreign relations, economy, public health, public safety, public order
Computer system targeted	Any computer system	CII; "an essential service"; threat to national security etc.; threat/incident of severe nature because of no. of persons, computers, value of info, whether or not computers/systems are CII	Essential service, national security, defence, foreign relations, economy, public health, public safety, public order
Information rights of commissioner	Interview any person, produce any information, copy any record, examine any acquainted person	Interview any person, produce any information, copy any record, examine any acquainted person (same as general threat)	• Require any person to provide any information – including design, configuration, operation, cybersecurity, description information • Provide with any info incl. real time • Report of breach/attempt

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS (SUMMARY)

	General Cybersecurity Threat (s.19)	Severe Cybersecurity Threat (s.20)	Critical Cybersecurity Threat (s.23)
Action		• Direct any person to carry out remedial measures, or cease action • Owner to take any action to assist in investigation • Enter premises after giving reasonable notice • Assess, inspect computer/system and check/search any data • Get assistance from any person • Scan for vulnerabilities • Take/extract any affected record/program • Take possession of any computer/equipment for further examination (even without consent)	• Take such measures as may be necessary • Power to access computer

RESPONSES TO CYBERSECURITY THREATS & INCIDENTS (SUMMARY)

	General Cybersecurity Threat (s.19)	Severe Cybersecurity Threat (s.20)	Critical Cybersecurity Threat (s.23)
Exemption	• Information subject to right, privilege, immunity, rules of conduct are exempted from production	• Same	• Government not allowed to ask for privileged documents, but if they do ask for it, there is no exemption from product. However, take note that immunity provided.
Immunity	• As long as reasonable care was taken and you act in good faith, any actions undertaken to comply with CSA will not constitute a breach of contract		• No liability for any acts taken in compliance with s 23. • No breach of legal, contractual or professional restriction
Offence	• Willfully misstates or without reasonable excuse refuses to give any information or comply with Magistrate's order: $5,000 or 6 months in jail or both	• Willfully misstates or without reasonable excuse refuses to give any information or comply with Magistrate's order, **or comply with direction or lawful demand**: $25,000 or 2 years in jail or both	• Without reasonable excuse fails to take any measure or comply with any requirement, or obstructs a specified person or fails to comply with any direction: $50,000 or 10 years in jail or both

BREAK

CYBERSECURITY ACT – LICENSING REGIME FOR CYBERSECURITY SERVICE

DEFINITION OF CYBERSECURITY SERVICE

- a service provided by a person for reward that is intended primarily for or aimed at ensuring or safeguarding cybersecurity of a computer/system belonging to another person, and includes:
  - assessing, testing or evaluating cybersecurity by searching for vulnerabilities/compromises in cybersecurity defences;
  - forensic examination of computer/system;
  - investigating and responding to a cybersecurity incident by conducting scan, examination, removal, identify root cause, circumventing controls;
  - conducting thorough examination to detect any cybersecurity threat or incident that may have penetrated cybersecurity defences or evaded detection;
  - designing, selling, importing, exporting, installing, maintaining, repairing or servicing of one or more cybersecurity solutions;

CYBERSECURITY ACT – LICENSING REGIME FOR CYBERSECURITY SERVICE

- monitoring cybersecurity by acquiring, identifying and scanning information for identifying cybersecurity threats;
- maintaining control of the cybersecurity of computer/system by effecting management, operational and technical controls;
- assessing or monitoring organisation compliance with cybersecurity policy;
- providing advice in relation to cybersecurity solutions, including —
  - a cybersecurity program; or
  - identifying and analysing cybersecurity threats and providing advice on solutions or management strategies to minimise the risk posed by cybersecurity threats;
  - any practices that can enhance cybersecurity;
  - providing training or instruction for any cybersecurity service, including assessment of the, instruction or competencies of another;

WHAT IS NOT A CYBERSECURITY SERVICE?

- cybersecurity service by a *company* to its related company: see definition, s 24(3)
- cybersecurity service by a company employee of its own computer/service: see definition
- cybersecurity service not as a standalone service and not "primarily for or aimed at" safeguarding cybersecurity: see definition
- cybersecurity service not provided "for reward": see definition

LICENSABLE CYBERSECURITY SERVICE

Second Schedule of the CSA

- managed security operations centre (SOC) monitoring service
  - a service for the monitoring of the level of cybersecurity of a computer/system of another person by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer/system for the purpose of identifying cybersecurity threats to the computer/system
- penetration testing service
  - a service for assessing, testing or evaluating the level of cybersecurity of a computer/system, by searching for vulnerabilities in, and compromising, the cybersecurity defences of the computer/system

LICENSING OF CYBERSECURITY SERVICE PROVIDERS

- Licence required to
  - provide "licensable cybersecurity service": s 24(1)(a)
  - advertise or hold out the provision of "licensable cybersecurity service": s 24(1)(b) • unlicensed service provider not entitled to recover fees: s 31
- Licence to be applied for and renewed: s 26
  - whether fit and proper person to hold/continue to hold licence
  - whether convicted of any offence, or as judgement entered against involving fraud, dishonesty, moral turpitude/breach of fiduciary duty
  - as individual: whether suffering from mental disorder, is undischarged bankrupt, entered into composition
  - whether officer of business is fit and proper person
  - as business: whether in liquidation or winding up, receiver appointed, composition/arrangement
  - whether had previously had licence revoked

LICENSING OF CYBERSECURITY SERVICE PROVIDERS

- Licence conditions: s 27
- Obligations
  - duty to keep records of client, person providing service, date, details of service: s 29(1)(a)
  - keep records for not less than 3 years: s 29(1)(b)
  - furnish records to licensing officer: s 29(2)
  - offence to make and furnish false/misleading record: s 29(3) ($10,000 or 12 months imprisonment or both)
  - no offence is record is not false or misleading in a material particular: s 29(4)
- Revocation of licence on breach of (usual) conditions: s 30, or subject to financial penalties - $10,000 for each contravention, max aggregate $50,000: s 32
- No recovery of fees if unlicensed: s 31; financial penalty may be ordered for contravention: s 32

EVALUATION OF THE CYBERSECURITY ACT

- Duties of Organizations
- Immunity provisions vs existing legal obligations
- Cost for general and specific compliance
- Breadth of CSA Commissioner's powers
- Organizational Management and Planning

IMMUNITY PROVISIONS

- Only exception is where information is protected by legal professional privilege: s 15A(3) (cf. s 19(6), 23(4), CSA)
- Non-compliance with measures or directions under s 15A, or obstruction from compliance "without reasonable excuse" is an offence: s 15A(4), (5) (cf. ss 19(6), (8), 20(7), 23(4), CSA)
- Good faith compliance immunizes of all persons (directly and indirectly) of all civil and criminal liability: s 15A(6), (7)
- Debates: "For example, if a malware is detected to be targeting a particular make and model of equipment used by our CII operators, the Minister may issue a certificate to the CII operators to direct that certain cybersecurity measures be taken. In the course of implementing these measures in good faith, if there is service degradation or disruption that results in the failure of the CII operators to meet their contractual Service Level Agreements with their customers, the CII operators can claim immunity in any legal proceedings against them by their customers." (cf. s 20 vs. s 23(6), (7))

MEASURES TO BE TAKEN BY COMPANY

- Q: So as an organization, what can you do to prepare yourself for managing such cybersecurity directions or requests under s 15A, CMCA (ss 19, 20, 23, CSA)?
  - segregation of essential from non-essential services
  - develop protocol for supply of information w/o disrupting provision of key sservices
  - proactively implement good cybersecurity measures
  - compliance with directions, but seek clarification when directions are vague and ambiguous
  - exercise good faith when complying with directions
  - document (and justify) your decisions!

WHERE DO WE GO FROM HERE WITH RECENT EVENTS? POST SINGHEALTH

Following SingHealth breach, the *Government's Response to the Report of the Committee of Inquiry into the Cyber Attack on SingHealth's IT System*:

- *First, we adopt a :defence-in-depth" strategy, with **multiple layers of cyber defences** to impede an attacker. These layers of defence cascade from the perimeter to within our systems, as we recognise that a sophisticated and determined attacker, given enough time and resources, may find a way through. This is why we also have capabilities in our layered defence that enable swift detection of a breach and a decisive response.*
- *Second, we seek to enhance our system defences by strengthening our **people, processes and technology**. Our aim is not only to monitor and respond robustly to an incident, but also to ensure a quick recovery and resilience in our system.*

WHERE DO WE GO FROM HERE?

Following Solar Wind breach, Minister *Iswaran*:

- *And therefore, the first and perhaps most important point is the **"zero-trust" posture that we must adopt**. In other words, always be vigilant, constantly evaluate our systems and conduct regular monitoring and threat hunting exercises. I think this is a **fundamental**; it is a posture that we need to adopt across not just our critical information infrastructure, but indeed **across all organisations**, especially as our digital footprint grows as we adopt new digital solutions.*
- *Secondly, on the part of CSA and the Government, CSA works with our CII sectors in particular, to **share information** regularly on evolving threats and also on solutions that are available for adoption. In particular, CSA is in regular contact with its counterparts around the world and that is an important source of this information and intelligence that is necessary to strengthen our own system. …*
- *Finally, CSA works with several private sector partners and others to ensure various forms of cybersecurity solutions are available for **adoption and use by not just the large enterprises and our CIIs but also SMEs**.*