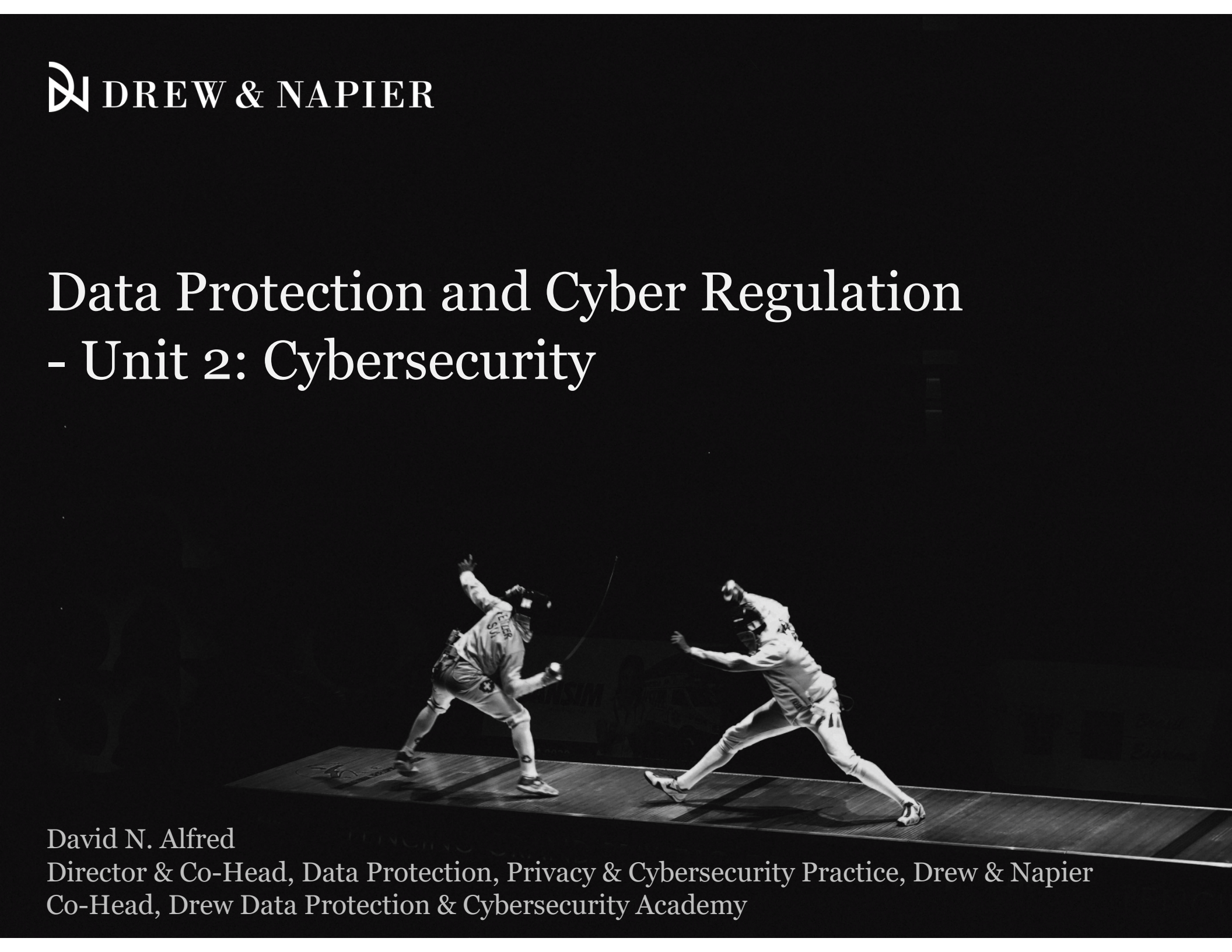
DREW & NAPIER

Data Protection and Cyber Regulation - Unit 2: Cybersecurity



David N. Alfred
Director & Co-Head, Data Protection, Privacy & Cybersecurity Practice, Drew & Napier
Co-Head, Drew Data Protection & Cybersecurity Academy

Topics Covered

1. Introduction to Cybersecurity
2. Cybersecurity Act 2018
3. Personal Data Protection Act 2012

Readings for this Unit

1. Cybersecurity Act 2018 (*CYSA*), Sections 7, 10 to 16, 19 and 20 and First Schedule
2. Cyber Security Agency, Cybersecurity Code of Practice for Critical Information Infrastructure, Section 3 (Governance Requirements)
3. Personal Data Protection Act 2012 (*PDPA*), Sections 24 and 26A to 26E
4. Personal Data (Notification of Data Breaches) Regulations 2021 (*DBNR*)
5. [2019] SGPDPC 3 Singapore Health Services Pte Ltd and Integrated Health Information Systems Pte Ltd
6. Personal Data Protection Commission (PDPC), Advisory Guidelines on Key Concepts in the Personal Data Protection Act (Strongly Recommended)

1 | Introduction to Cybersecurity

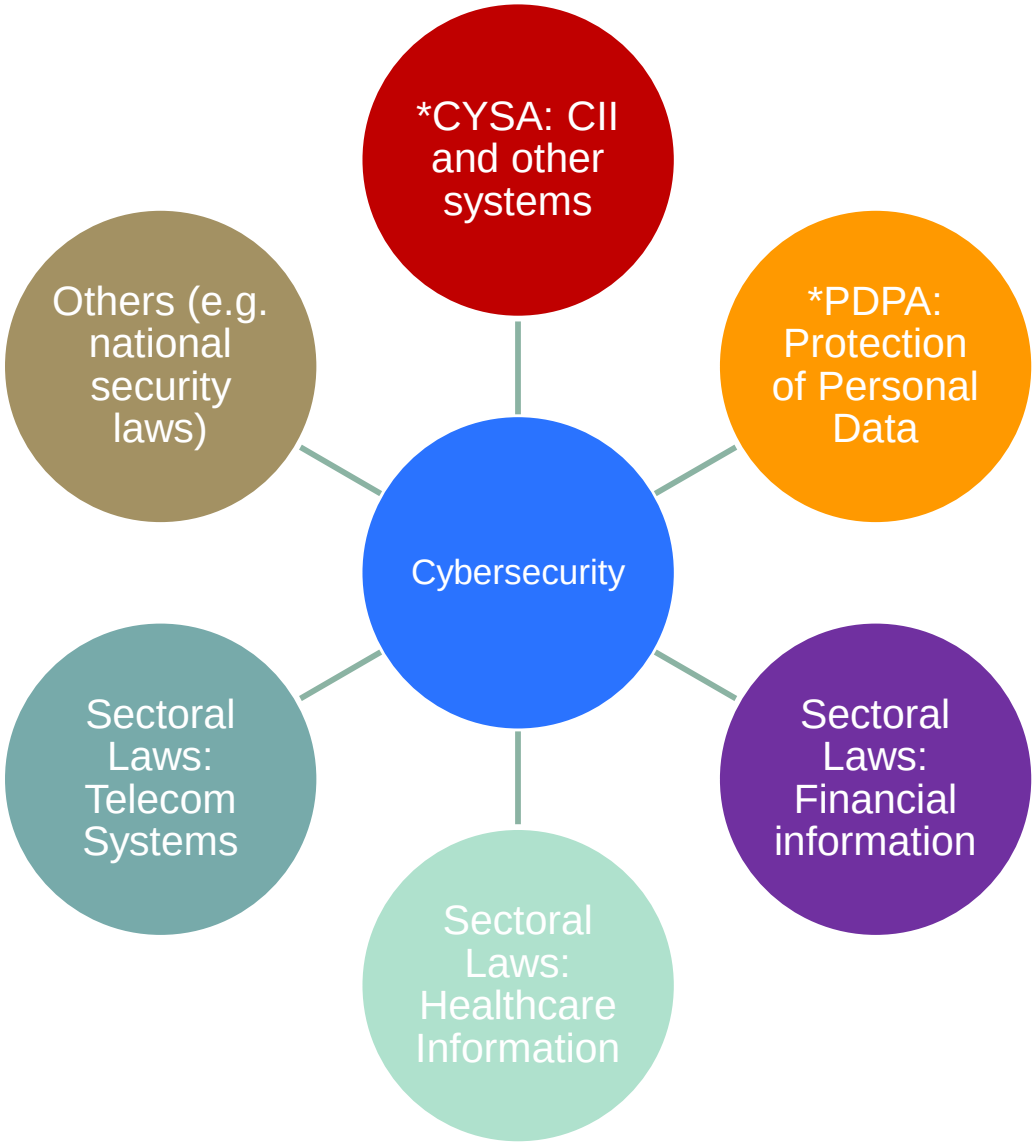
Cybersecurity as Part of Total Defence

Some starting questions

1. What is cybersecurity?
   - "Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks" (Source: Kaspersky website)
   - Protecting confidentiality, integrity and availability of systems and data (the "CIA" of cybersecurity)
   - Resilience of systems
   - Other definitions?

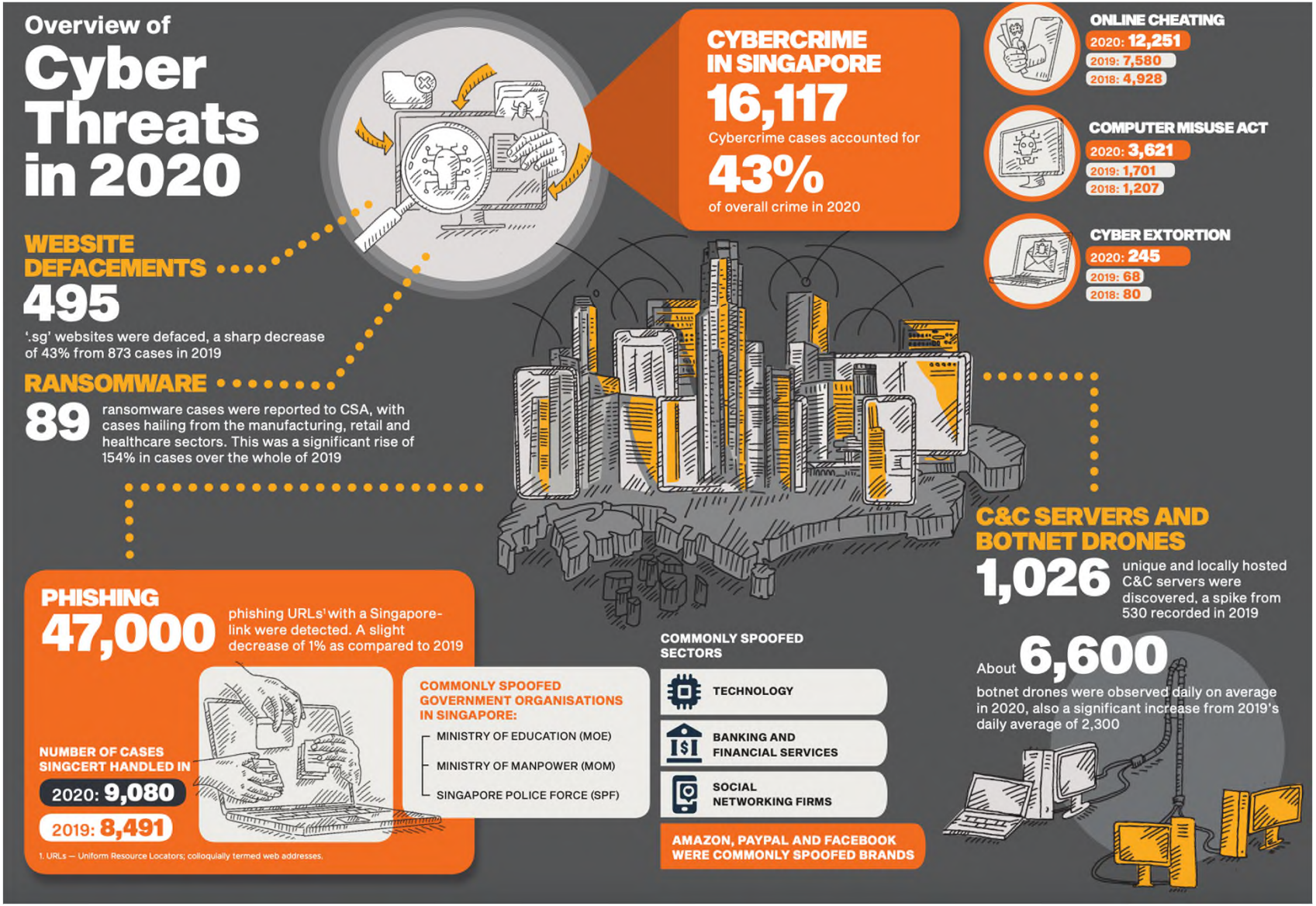
2. What is cybersecurity law?
   - Laws that regulate how businesses and other organisations:
     - protect their computer systems and data from cyber-attacks
     - Respond to cyber-attacks and data breaches

Laws that Regulate Cybersecurity



*We are focusing on the CYSA and the PDPA

Why regulate cybersecurity?



Why regulate cybersecurity?

- Significant increase in number of cyberattacks in recent years
- Some motivations of cyber-criminals:
  - Organised crime – to make a profit from their criminal activities
  - Corporate cyber-espionage
  - State actors
  - Individual reputation
  - Cyber-activism (Hacktivism)

Why regulate cybersecurity?

- Numerous types of malware:
  - Ransomware - Hit 65% of organisations in Singapore in 2021 (source: Sophos)
  - Trojans
  - Viruses
  - Spyware
  - Worms
  - Adware
- Phishing
- Hacking
- Botnets & DDoS attacks
- Identity Theft
- Website Spoofing

How does a cyber-attack take place?

Singapore Health Services & Integrated Health Information Systems [2019] SGPDPC 3

- What were the facts of this case (in brief)?
- What was the relationship between SingHealth and IHiS ?
- What were the steps / actions taken by the hacker to gain access to the system and data?
- How did SingHealth and IHiS staff respond in the course of the incident?
- What were the specific security shortcoming identified by the Personal Data Protection Commission in its decision?

2| CYBERSECURITY ACT 2018

PART 1: INTRODUCTION

Purpose and Overview

- Cybersecurity Act 2018, Long title:
  - An Act
    - to require or authorise the taking of measures to **prevent, manage and respond to cybersecurity threats and incidents**
    - to **regulate owners of critical information infrastructure**
    - to **regulate cybersecurity service providers**
- Provisions:
  - Part 1 – Preliminary
  - Part 2 – Administration (appointment of Commissioner of Cybersecurity, etc.)
  - Part 3 & First Schedule – **Critical Information Infrastructure** (“**CII**”)
  - Part 4 – **Responses to Cybersecurity Threats and Incidents**
  - Part 5 & Second Schedule – **Regulation of Cybersecurity Service Providers** **[not covered in this unit]**

Scope

- Part 3 applies to:
  - any **CII** wholly or partly in Singapore (per s 3(1))
  - any **computer or computer system** wholly or partly in Singapore (per s 3(2))
- Part 4 applies to activities and service providers in Singapore generally

Key Definitions (Section 3)

- **CII**: a computer or a computer system designated under s 7(1)
- **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 …"
  - Excludes prescribed devices (none at present)
- **Computer System**: an arrangement of interconnected computers and includes:
  - "an information technology system"
  - "an operational technology system such as an industrial control system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system"

Key Definitions (Section 3)

- **Cybersecurity**: The state in which a computer or computer system is protected from unauthorised access or attach such that the following is maintained (note: the "CIA" of cybersecurity):
  - **Confidentiality** of information processed, etc. by the computer or computer system (what about the computer / system itself?)
  - **Integrity** of the computer or computer system or the information it processes, etc.
  - **Availability** of the computer or computer system (and information?)
- **Cybersecurity Threat**: "an act or activity (whether known or suspected) carried out on or through a computer or computer system, that **may imminently jeopardise or affect adversely**, without lawful authority, the cybersecurity of that or another computer or computer system"
- **Cybersecurity Incident**: "an act or activity carried out without lawful authority on or through a computer or computer system that **jeopardises or adversely affects** its cybersecurity or the cybersecurity of another computer or computer system"

Key Definitions (Section 3)

- **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”
- Essential services in the First Schedule include:
  - Aviation, Land Transport or Maritime
  - Banking and Finance
  - Energy or Water
  - Info-communications or Media
  - Functioning of Government
  - Security and Emergency Services
  - Healthcare

PART 2: REGULATION OF CII

Regulation of CII

(I) Designation of CII (s 7)

- The Commissioner may obtain information from a person who appears to be exercising control over a computer or computer system for the purpose of ascertaining whether it is fulfills the criteria of a CII (s 8(2))
  - Failure to comply is an offence (s 8(4))
  - Same exception for legal privilege as s 19
- The Commissioner may designate a computer or computer system as CII if both of the following apply (s 7(1)):
  - the computer or computer system is **necessary for the continuous delivery of an essential service**, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore
  - the computer or computer system is **located in Singapore** (Q: what about cloud-based services?)

Regulation of CII

(I) Designation of CII (s 7, continued)

- A designation under s 7(1)
  - must *inter alia* inform the owner of the CII of the owner's duties and responsibilities under the CYSA that arise from the designation (s 7(3))
  - is valid for 5 years (s 7(3))
- See also sections 8 and 9; additional procedures are found in the Cybersecurity (Critical Information Infrastructure) Regulations 2018 [not covered]

Regulation of CII

(II) Obtaining Information Relating to a CII (ss 10, 12 & 13)

- The Commissioner may require the owner of a CII to furnish the following information (s 10(1)):
  - Information on the design, configuration and security of the CII or any other computer or computer system under the CII owner's control that is interconnected or communicates with that CII
  - Information relating to the operation of that CII or other computer or computer system
  - Any other information in order to ascertain the level of cybersecurity of the CII
- Material changes to the design, configuration, security or operation are to be updated within 30 days (s 10(5))
- Any change in the beneficial or legal ownership must be notified to the Commissioner with 7 days by the former owner, if the whole ownership is transferred, or otherwise any owner of the CII (s 13(1))
- Failure to comply with any of the above is an offence (ss 10(2), 10(7) & 13(2))
- Same exception for legal privilege, etc. as s 19

Regulation of CII

(III) Codes of Practice and Standards of Performance (s 11)

- The Commissioner may issue or approve one or more codes of practice or standards of performance for the regulation of the owners of CII with respect to measures to be taken by them to ensure the cybersecurity of the CII (s 11(1)(a))
- Every owner of a CII **must comply with the codes of practice and standards of performance** that apply to their CII (following publication of a notice relating to the code or standard) unless otherwise waived by the Commissioner under s 11(7) (s 11(6))
- The Commissioner may amend or revoke any code of practice or standard of performance (s 11(1)(b)))
- The Commissioner must publish a notice of the issuance, approval, amendment or revocation of a code of practice or standard of performance (s 11(3)) failing which it does not take effect (s 11(4))
- A code of practice or standard of performance does not have legislative effect (s 11(5)) and any of its provisions that is inconsistent with the CYSA does not have effect (to the extent of the inconsistency) (s 11(2))
- The Commissioner for Cybersecurity / CSA issued the Cybersecurity Code of Practice for Critical Information Infrastructure on 4 July 2022, last updated 12 Dec 2022 (https://www.csa.gov.sg/legislation/codes-of-practice)

Regulation of CII

(IV) Directions to Ensure Cybersecurity of a CII (s 12)

- The Commissioner may issue a direction to the owner(s) of a CII in order to ensure the cybersecurity of the CII or it is necessary or expedient for the administration of the CYSA (s 12(1))
- Without limitation, a direction may include the following (s 12(2)):
  - the **action to be taken by the owner(s) in relation to a cybersecurity threat**
  - **compliance with any code of practice or standard of performance** applicable to the owner(s)
  - appointment of an **auditor** approved by the Commissioner to audit the owner(s) on their compliance with the CYSA or any code of practice or standard of performance applicable to the owner(s)
- Process for issuance of a direction includes giving the owner an opportunity to make representations (s 12(4) & (5))
- Failure to comply is an offence (s 12(6))

Regulation of CII

(V) Duty to Report Cybersecurity Incident in respect of CII (s 14)

- The owner of a CII must notify the Commissioner upon the occurrence of any of the following (s 14(1)):
  - a **prescribed cybersecurity incident** in respect of the CII or any other computer or computer system under the CII owner's control that is interconnected with or that communicates with the CII
  - any other type of cybersecurity incident in respect of the CII that the Commissioner has **specified by written direction** to the owner
- The owner of a CII must establish such **mechanisms and processes for the purposes of detecting** cybersecurity threats and incidents in respect of the CII, as set out in any applicable code of practice (s 14(2))
- Failure to comply is an offence (s 14(3))

Regulation of CII

(VI) Cybersecurity Audits and Risk Assements (s 15)

- The owner of a CII must comply with the following (s 15(1)):
  - at least once every 2 years, cause an audit to be carried out of the compliance of the CII with the CYSA and the applicable codes of practice and standards of performance (to be done by an auditor approved or appointed by the Commissioner)
  - at least once a year, conduct a cybersecurity risk assessment of the CII
- The owner of a CII must furnish a copy of the audit report or risk assessment to the Commissioner within 30 days of completion (s 15(2))
- See the rest of the section for further details
- Failure to comply is an offence (s 15(7) & (8))

Regulation of CII

(VII) Cybersecurity Exercises (s 16)

- The Commissioner may conduct cybersecurity exercises for the purpose of **testing the state of readiness** of owners of different CII in responding to significant cybersecurity incidents.
- An owner of a CII must participate in a cybersecurity exercise if directed in writing to do so by the Commissioner
- Failure to comply is an offence (s 15(7) & (8))

PART 3: RESPONSE TO CYBERSECURITY THREATS AND INCIDENTS

Response to Cybersecurity Threats and Incidents (CYSA, Part 4)

(I) Investigation (s 19)

- The Commissioner may investigate any cybersecurity threat or incident for the following purposes (s 19(1)):
  - assessing the impact or potential impact of the cybersecurity threat or incident
  - preventing harm arising from the cybersecurity incident
  - preventing a further cybersecurity incident from arising from that cybersecurity threat or incident
- The Commissioner's powers of investigation (s 19(2)) may be applied as against any person (e.g. to compel attendance and obtain information) and failure to comply is an offence (s 19(8))
- Legal Privilege, etc.: Disclosure of information that is subject to any right, privilege or immunity conferred, or obligation or limitation imposed, by or under any law or rules of professional conduct in relation to the disclosure of such information is **not required**, except that the performance of a contractual obligation is not an excuse for not disclosing the information (s 19(6))

Response to Cybersecurity Threats and Incidents (CYSA, Part 4)

(II) Elimination of Serious Threats and Incidents (s 20)

- The Commissioner has additional powers in relation to any cybersecurity threat or incident that meets any of the following criteria (s. 20(3)):
  - it creates a risk of significant harm being caused to a CII
  - it creates a risk of disruption to the provision of an essential service
  - it creates a threat to the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore
  - it is of a severe nature, in terms of the severity of the **harm that may be caused to persons** in Singapore or the **number** of computers or **value** of the information put at risk, whether or not the computers or computer systems put at risk are themselves CII
- The Commissioner may investigate any such serious cybersecurity threat or incident for the following purposes (s 20(1)):
  - assessing the impact or potential impact of the cybersecurity threat or incident
  - **eliminating the threat** or preventing harm arising from the cybersecurity incident
  - preventing a further cybersecurity incident

Response to Cybersecurity Threats and Incidents (CYSA, Part 4)

(II) Elimination of Serious Threats and Incidents (s 20, continued)

- For such serious cybersecurity threats and incidents, the Commissioner may:
  - in addition to the powers under s 19(1)
  - direct, (by written notice) any person to carry out **remedial measures**, or to cease carrying on certain activities in relation to a computer or computer system that […] is or was affected by the cybersecurity incident, in order to minimise cybersecurity vulnerabilities in the computer or computer system
  - require the owner of a computer or computer system to take any action to assist with the investigation (examples in the Act)
  - enter premises, perform scans, obtain records, etc.
- Examples of remedial measures (under s 20(2)) include the following:
  - removal of malicious software from the computer;
  - installation of software updates to address cybersecurity vulnerabilities;
  - temporarily disconnecting infected computers from a computer network until the above is carried out
  - redirection of malicious data traffic towards a designated computer or computer system

Introduction

- The PDPA, Singapore's first general data protection law, was enacted in 2012 and came into force in stages up to July 2014
  - Personal Data Protection Commission (PDPC) was established in 2013
  - PDPA's Do Not Call and Data Protection Provisions came into force in 2014
- PDPA was significantly amended in 2020 to introduce new obligations in line with modern data protection laws in other jurisdictions
  - New provisions on data protection obligations and rights of individuals
  - New criminal offences relating to misuse of personal data
  - Enhanced enforcement powers for PDPC/Commissioner

PART 4: CYBERSECURITY CODE OF PRACTICE

Overview

- Topics covered in the Cybersecurity Code of Practice for CII ("**COP**"):
  - Audit requirements
  - Governance requirements
  - Identification requirements (Asset Management)
  - Protection requirements
  - Detection requirements
  - Response and Recovery requirements
  - Cyber Resiliency requirements
  - Cybersecurity Training & Awareness
  - Operational Technology (OT) Security requirements
  - Domain-specific requirements (DNSSEC)
- We are only focussing on Governance requirements (section 3 of the COP)
- Note relevant definitions

Governance of Cybersecurity

- Key requirements in the COP, Section 3:
  - Leadership and oversight
    - Adequate resources to cybersecurity strategy and application to CII
    - Effective leadership from the board and senior management
  - Risk management
    - Risk management framework to identify, analyse, evaluate and address (respond to) cybersecurity risks in a cost-effective manner
    - Maintain a risk register for each CII
  - Policies, Standards, Guidelines and Procedures
    - Policies and standards for (internal) compliance
    - Guidelines on best practices
    - Procedures with specific actions to be taken
  - Security-by-Design, Cybersecurity Design Principles and Change Management are not covered

Governance of Cybersecurity

- Key requirements in the COP, Section 3 (continued):
  - Use of Cloud
    - Organisation remains responsible for maintaining oversight of cybersecurity and managing cybersecurity risks to CII even if CII is wholly or partly implemented using cloud computing systems
  - Outsourcing and vendor management
    - Organisation remains responsible for cybersecurity even if it engages an external party to perform any functions with respect to the CII
    - Controls must be implemented to minimise cybersecurity risks

3| PERSONAL DATA PROTECTION ACT 2012

Overview

- Data Protection obligations previously covered in unit 1
- Today, we are focusing on:
  - Protection (security) of personal data
  - Data breach notification

PART 1: PROTECTION OF PERSONAL DATA

Protection of Personal Data (Section 24)

- Although data protection laws predated the advent of the Internet and the wide-spread use of computing devices we have today, they typically included a specific obligation to protect personal data
- Under the PDPA, all organisations are required to protect personal data by making reasonable security arrangements to prevent the following (s 24):
  - unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks
  - loss of any storage medium or device on which personal data is stored
- In a modern context, as most data is stored in electronic form in computers, computer systems and other electronic / digital devices and systems, this translates to requirements to ensure cybersecurity of systems and databases containing personal data

Protection of Personal Data (Section 24)

- Requirements:
  - Covers personal data in the possession or under the control of the organisation
  - "reasonable security arrangements" – not defined (Side note: This kind of wording is found in many other countries law including, e.g. EU and US)
  - Two key elements, measures are to prevent:
    - unauthorised access, etc. to personal data
    - loss of storage media / devices containing personal data

Protection of Personal Data (Section 24)

- PDPC's Advisory Guidelines on Key Concepts in the PDPA, para 17
  - "There is no 'on size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances …"
  - Factors to take into consideration:
    - Nature of the personal data
    - Form in which the personal data was collected (e.g. electronic or physical)
    - Possible impact to the individual concerned if an unauthorised person obtains, modifies or disposes of the personal data

Protection of Personal Data (Section 24)

- PDPC's Advisory Guidelines on Key Concepts in the PDPA, para 17 (continued):
  - In practice, an organisation should:
    - Design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that may result from a security breah
    - Identify reliable and well-trained personnel responsible for ensuring information security
    - Implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity
    - Be prepared and able to respond to information security breaches promptly and effectively
  - Security arrangements include:
    - **Administrative measures** (e.g. confidentiality obligations, robust policies, staff training)
    - **Technical measures** (e.g. network security measures, access control, use of encryption)
    - **Physical measures** (e.g. physical locks, privacy filters, proper disposal of physical documents)

Protection of Personal Data (Section 24)

- In relation to data intermediaries and the organisations that engage them (data controllers), note that section 24 applies to both (per S. 4(2) & (3))
- Scope of responsibility depends on extent of tasks to be done by each:
  - Processing by the data intermediary (implement necessary technical, physical and administrative measures)
  - Governance by the data controller (implement, typically via contract, measures to govern the data intermediary's protection of personal data)

PART 2: DATA BREACH NOTIFICATION

Scope

- Definition/Concepts (Ss 26A & 26B):
  - **Data Breach**: (a) unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data, or (b) loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur
    - Cf. s 24
  - **Notifiable Data Breach**: A data breach that (a) results in, or is likely to result in, significant harm to an affected individual or (b) is, or is likely to be, of a significant scale
    - A data breach is deemed to result in significant harm and is deemed to be of significant scale in prescribed circumstances (s 26B(2) & (3))
    - Significant harm: see Personal Data Protection (Notification of Data Breaches) Regulations 2021 ("**DBN Regulations**"), reg. 3 and Schedule (see next slide)
    - Significant scale: 500 (see DBN Regulations, reg. 4)
    - Notwithstanding the above, a data breach within an organisation is not notifiable (s 26B(4))

DBN Obligations

(I) Conduct an Assessment of a Data Breach

- Where an organisation has reason to believe that a data breach has occurred affecting personal data in its possession or under its control:
  - If the organisation is a data intermediary and the affected data is data it is processing for the data controller, the organisation (DI) must notify the data controller of the data breach without undue delay (s 26C(3))
  - If the organisation is a data controller, in must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach (s 26C(2))
- Q: Timeframes?
- Also note obligation of a data intermediary of a public agency (s 26E)

DBN Obligations

(II) Notification to PDPC

- Where an organisation assess that a data breach is notifiable, it must notify PDPC as soon as practicable and, in any case, within 3 calendar days (s 26D(1))
- Notification to PDPC is to be made via the PDPC website (www.pdpc.gov.sg)
- The notification must contain the prescribed information, to the best of the knowledge and belief of the organisation when the notification is made (s 26D(3))
  - The specific information required is set out in the DBN Regulations (reg. 5) and the relevant webform on the PDPC website
- Notification to PDPC (and affected individuals – see next slide) apply concurrently with any other obligation of the organisation to notify any other person (e.g. CSA) of the occurrence of a data breach

DBN Obligations

(III) Notification to Affected Individuals

- Where an organisation assess that a data breach is notifiable and it results, or is likely to result, in significant harm to the affected individuals, it must also notify the affected individuals on or after notifying PDPC (s 26D(2))
- Notification to the affected individuals is to be made in any manner that is reasonable in the circumstances (s 26D(2))
- The notification must contain the prescribed information, to the best of the knowledge and belief of the organisation when the notification is made (s 26D(3))
  - The specific information required is set out in the DBN Regulations (reg. 6)

DBN Obligations

(III) Notification to Affected Individuals (continued)

- Exceptions to this requirement:
  - If the organisation, on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual (s 26D(5)(a))
  - If the organisation had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual (s 26D(5)(b))
  - If a prescribed law enforcement agency so instructs or PDPC so directs (s 26D(6))
  - PDPC, on application by the organisation, waives this requirements (s 26D(7))

Drew & Napier LLC
10 Collyer Quay, #10-01 Ocean Financial Centre, Singapore 049315
www.drewnapier.com