

Overview of Legislations on

# Cybersecurity, Personal Data Protection & Computer Misuse





## Purpose

Digitalisation has changed the way we live and work, and along with that, the threats we face in the cyberspace. In Singapore, the government manages the issues of cybersecurity, data protection and computer misuse through three main pieces of legislation. This handbook seeks to explain the differences between the Cybersecurity Act, the Personal Data Protection Act, and the Computer Misuse Act in an easy to understand manner, so that organisations and individuals can do their part in being vigilant to protect their systems and devices.

### 01 Chapter 1

Introduction to Cybersecurity, Data Breach and Unauthorised Access and Modification to Computer Material

### 03 Chapter 2

Legislations in Singapore that govern Cybersecurity, Personal Data Protection and Computer Misuse

### 09 Chapter 3

Case Studies: Agency to approach for reporting of incident

### 17 Chapter 4

Initiatives and resources to help organisations and individuals better secure their computer systems

# Introduction to Cybersecurity, Data Breach and Unauthorised Access and Modification to Computer Material



## Cybersecurity

A state in which a computer or computer system is protected from unauthorised access or attack, so that they remain available, operational, and the integrity and confidentiality of information stored within remains intact.



## Data Breach

An incident exposing personal data in an organisation's possession or under its control to the risks of unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.



## Unauthorised access to computer material and unauthorised modification of computer material

### Unauthorised access to computer material

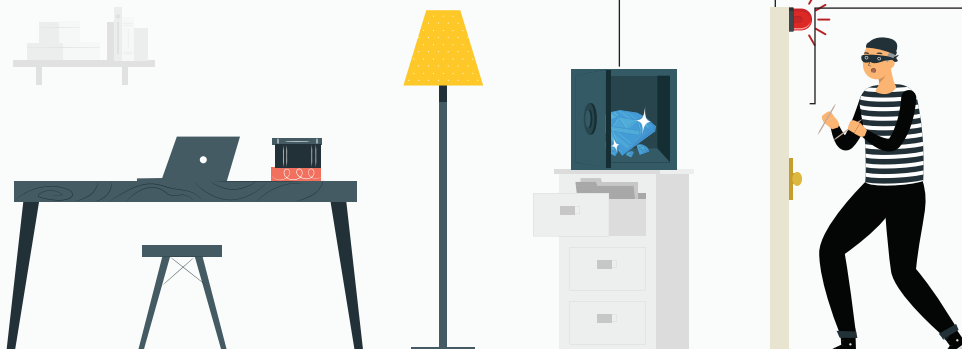
An act committed by a person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any computer program or data. This is also commonly known as "hacking".

### Unauthorised modification of computer material

An act committed by a person who knowingly causes unauthorised modification of the contents of any computer, e.g. introduction of viruses, ransomware or malware into the computer system or defacement of a webpage. Such an act usually causes the contents of the computer to be altered and/or impairs the normal operations of the computer.

## Consequences of inadequate measures put in place:

Inadequate measures could cause a debilitating effect on the availability of essential services in Singapore, damage to reputation, loss of trust, confidentiality, integrity, availability of information and financial losses for organisations and individuals. While the legislations seek to protect the online safety of organisations and individuals, a safer cyberspace can only be achieved when everyone plays their part. Good cybersecurity practices, tight access control and data protection mechanisms, strong passphrases and updated security policies help in ensuring that proprietary information is protected from exfiltration, intentional disclosure, modification, erasure or copying.



## Legislations in Singapore that govern Cybersecurity, Personal Data Protection and Computer Misuse

### Cybersecurity Act ("CS Act")

Administered by the Cyber Security Agency of Singapore ("CSA")

**The Cybersecurity Act** was established in 2018 to provide a legal framework for the oversight and maintenance of national cybersecurity in Singapore. Its four key objectives are to:

- 01 **Strengthen the protection of CII against cyber-attacks**
- 02 **Authorise CSA to prevent and respond to cybersecurity threats and incidents**
- 03 **Establish a framework for sharing cybersecurity information**
- 04 **Establish a licensing framework for cybersecurity service providers**



Cybersecurity is a key enabler in Singapore's transformation journey into a Smart Nation. It allows us to leverage on the digital opportunities available with a peace of mind. A robust cybersecurity environment is crucial for trusted and secure use of technology and enable our digital economy to flourish. Cybersecurity is a collective responsibility — from individuals to enterprises to the government, all stakeholders can and must play a role.

Cyber-attacks on Singapore's essential services can result in disruptions which could cripple our economy, and potentially lead to loss of life. Critical Information Infrastructure ("CII") are computer systems directly involved in the provision of essential services.



Owners of a computer system which are designated as a CII must put in place cybersecurity measures to ensure their systems are cyber resilient and protect them against cyber-attacks. CS Act imposes obligations on CII owners involved in the provision of essential services in Singapore. It aims to enhance the protection of these systems which in the event of loss or compromise would have a debilitating effect on the availability of the essential services in Singapore. These essential services relate to Energy, Info-communications, Water, Healthcare, Banking and Finance, Security and Emergency, Aviation, Land Transport, Maritime, Media and Government.

CII owners, amongst other obligations, are obliged to inform the Commissioner of Cybersecurity of any change in ownership of the CII, furnish information relating to the CII, conduct regular risk assessment and audit, report cyber incidents within a prescribed period and participate in cybersecurity exercises.

CS Act also authorises CSA to investigate and respond to cyber incidents. In the event of a cybersecurity threat or incident, CSA will assess the impact or potential impact and take appropriate action to prevent any or further harm arising from the threat or incident. For serious and imminent threat to CII or national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, emergency cybersecurity measures and requirements may be taken.



Scan here for more information

## | Personal Data Protection Act ("PDPA")

Administered by the Personal Data Protection Commission ("PDPC")



Today, vast amounts of personal data are collected, used and analysed, and this trend is set to continue growing exponentially. With more data generated, the higher the risks and larger the scale of personal data breaches occurring. A data protection regime is required to strengthen data protection for consumers and enable organisations to use data responsibly.

It recognises both the rights of individuals to protect their personal data, and the needs of organisations to collect, use or disclose such data for legitimate and reasonable purposes.



**PDPA** was established in 2012 as a baseline data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. The PDPA was amended in 2020, with enhancements to strengthen consumer trust that their data will be used responsibly as well as to enable organisations to confidently harness personal data for innovation.



Scan here for  
more information



PDPA requires all organisations that collect personal data to put in place measures for data protection. Such measures include the appointment of a Data Protection Officer ("DPO") to oversee the organisation's compliance to the PDPA, put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure or similar risks and to notify PDPC and affected individuals of a data breach that is likely to result in significant harm or impact to individuals, and/or is of a significant scale.

For breach of PDPA obligations, PDPC will commence investigation against organisations and may take enforcement actions such as directions, undertaking or imposition of financial penalties.

## Computer Misuse Act (“CMA”)

Administered by the  
Singapore Police Force (“SPF”)



**CMA** was enacted in 1993 to criminalise unauthorised access or modification of computer material, and other computer crimes. The Act governs the investigation and prosecution of cybercrime perpetrators.



Scan here for  
more information



As computer use becomes widespread, the risk of abuse becomes greater with criminals increasingly conducting their activities in the cyberspace. Before the introduction of the CMA, computer or computer-assisted crimes reported to the Police were dealt with under existing laws, such as the Penal Code. However, it became increasingly difficult to proceed under the general laws due to the complexities of computer technology.

Between 2013 and 2018, the CMA was renamed as the Computer Misuse and Cybersecurity Act and amended to allow for effective and timely measures against cyber threats that may endanger national interests or security. The legislation returned to its original name — CMA after the operationalisation of the CS Act in 2018.



CMA deals with the investigation and prosecution of cyber criminals. It criminalises offences such as hacking into a system, Denial of Service (DoS) attacks and *Wireless Mooching* or *Piggybacking*, etc. CMA also provides for enhanced punishment against offences that involves protected computers.



“Wireless Mooching” or “Piggybacking” refers to the act where one uses another person’s Wi-Fi connection without their consent.

## Case Studies: Agency to approach for reporting of incident

### CASE STUDY 01: SUPPLY CHAIN VULNERABILITIES



A cybersecurity researcher discovered that he could access personal data in a database through an online server and alerted PDPC to the matter. The database contained sensitive personal data of some 100,000 individuals belonging to Think Medical — a CII owner.

It was established that the vendor of Think Medical was tasked to update these sensitive data into Think Medical's off-site systems but had improperly placed them in an unsecured online database which was not patched or updated. Think Medical was not aware nor had they given agreement for the data to be placed on a server accessible through the Internet.

After Think Medical was alerted to the security lapse, the database was removed from the Internet and fully secured within an hour.

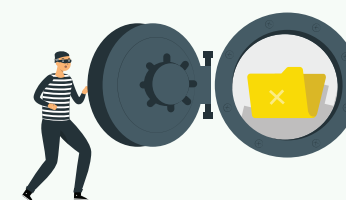


#### Agencies to notify



#### CSA

The cyber incident did not directly involve Think Medical's computer systems however the security lapse exposed its database containing sensitive personal data, thus the incident should be reported to CSA.



#### PDPC

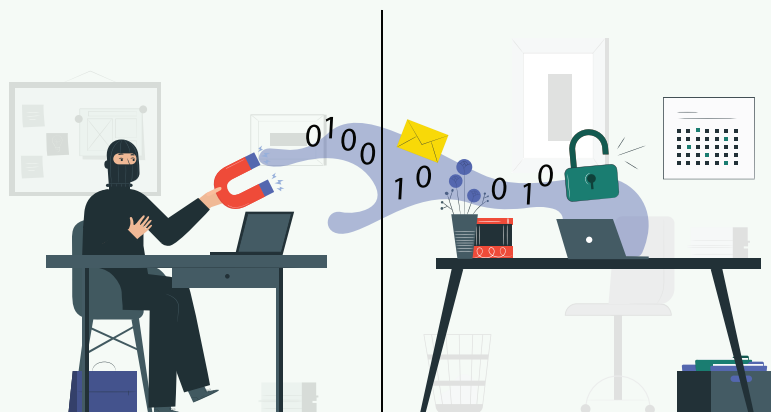
The personal data of 100,000 individuals was exposed, which is of significant scale, thus the PDPC must be notified.

#### Learning Point



Computer systems and data may be compromised through improper handling or poor cybersecurity practices by third party vendors. Organisations should factor cyber risk (including third party vendor risk management) as an organisation risk to be integrated within the overall business strategy and risk assessment so that measures may be implemented to mitigate such risks.

## CASE STUDY 02: THE SOPHISTICATED CYBER ATTACK



ICPT is a CII owner and its computer systems contained databases that have sensitive information belonging to citizens of Singapore. ICPT made changes to its systems and networks setup but did not inform CSA.

Months after the changes were made, ICPT's IT administrators began to notice unauthorised access to the servers that housed the databases but did not report the matter to CSA as they tried to resolve the issue internally. CSA was only informed two weeks later. By then, the attacker had successfully gained access to the databases and exfiltrated the personal data of over 100,000 individuals.

It was established that the changes made to the systems resulted in a vulnerability that was exploited by the attacker. Login passwords to the databases were also stored in cleartext within the system.

### Agencies to notify



CSA



PDPC



SPF



#### CSA

The cyber incident directly involves ICPT's computer systems and ICPT being a CII owner, needs to report the incident to CSA within the stipulated timeframe in accordance to the Cybersecurity (Critical Information Infrastructure) Regulations 2018.



#### PDPC

The personal data of 100,000 individuals was exfiltrated, which is of significant scale, and may pose significant harm to individuals, thus the PDPC must be notified.



#### SPF

There was unauthorised access to ICPT's computer systems thus a Police report should be lodged.



### Learning Point



CII owners that encountered cyber incident should report to the relevant authorities as soon as possible. This could prevent further attacks to the systems and help mitigate the situation. Having poor cybersecurity habits like common passwords, storing passwords in cleartext and weak access control could lead to disastrous consequences.

Change to systems and networks setup is a material change under the CS Act and it is the obligation of the CII owner to inform the Commissioner of Cybersecurity of the change. Failure to do so would constitute an offence in the CS Act.



## CASE STUDY 03: RANSOMWARE ATTACK



A system administrator in Sing Water Pte Ltd discovered that he could not access the folders and files in their web server and reported the issue to his IT department. Upon investigation, it was discovered that all systems including servers and user desktops were infected with ransomware. All folders, files and backups were encrypted. A ransom note was found in Sing Water Pte Ltd's server demanding a ransom to decrypt the files.

The threat actor also managed to gain access to their systems and exfiltrated sensitive information on Sing Water Pte Ltd's operations and computer systems. Personal data of individuals were not exfiltrated or tampered with.

### Agencies to notify



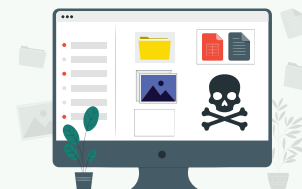
CSA



PDPC



SPF



### CSA

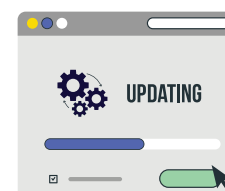
Though Sing Water Pte Ltd is not a CII owner, it should still report the incident to the Singapore Computer Emergency Response Team (SingCERT). This will enable SingCERT to understand the scope and nature of the incident, as well as alert and assist a broader range of individuals and organisations.

### SPF

There was unauthorised access to Sing Water Pte Ltd's computer systems thus a Police report should be lodged.



### Learning Point



Cyber criminals commit crimes for a variety of reasons. Prevention is key to avoid falling victim to cyber incidents such as ransomware. Even if you think that there is nothing of value to steal from your systems, failure to protect them may result in embarrassment and reputational losses to your organisation. Organisations need to take appropriate measures to secure their infrastructure and systems. It is also essential to formulate a backup and recovery plan for critical data, perform data backups regularly, and make sure that these are stored offline and not connected to your network.

## CASE STUDY 04: INSIDER THREAT



A disgruntled employee of ABC Gym exploited an administrator account with weak password that belonged to an ex-employee. With the administrator's privilege, the employee gained access to ABC Gym's database, downloaded personal data belonging to approximately 600 members and sold the information online for his personal gain. The employee's action was uncovered when a check was conducted on the company's system logs.

ABC Gym did not appoint a DPO to implement data protection policies within the organisation. It was also discovered that the ex-employee's account was not removed even though he left the organisation a year ago.

### Agencies to notify

○ CSA

✓ PDPC

✓ SPF



#### PDPC

The personal data of 600 individuals was leaked, which is of significant scale, thus the PDPC must be notified.



#### SPF

There was unauthorised access to ABC Gym's computer systems thus a Police report should be lodged.



### Learning Point



Implementing appropriate cybersecurity measures, such as maintaining access control, use of strong passphrases and enabling Multi-Factor Authentication can help prevent unauthorised access into computer systems and secure critical data. Organisations should also appoint a DPO to ensure they are compliant to the PDPA.

## Initiatives and resources to help organisations and individuals better secure their computer systems



### Initiatives and Resources for Organisations



#### SG Cyber Safe Programme

CSA's SG Cyber Safe Programme comprises a suite of initiatives to help Singapore enterprises raise their cybersecurity posture. These include **cybersecurity toolkits for business leaders, IT teams and employees**. The **SG Cyber Safe Trustmark**, complemented by a mark of **cyber hygiene**, are different forms of cybersecurity certification for enterprises. CSA will also partner the industry to further drive cybersecurity awareness through the **SG Cyber Safe Partnership Programme**.



Scan here for  
more information

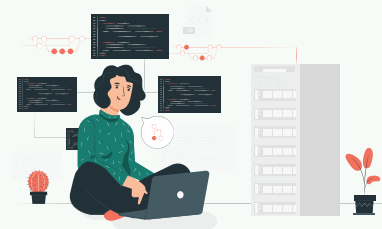


#### Singapore Common Criteria Scheme

The Common Criteria, also known as ISO/IEC 15408, is a globally recognised technical standard for IT security evaluation of commercial IT products targeting the international marketplace. The **Singapore Common Criteria Scheme is owned and managed by CSA**, and Singapore has been recognised as a Common Criteria Certificate Authorising Nation since January 2019. Through this initiative, products are evaluated and certified based on international standards to reduce the attack surface for the adversary.



Scan here for  
more information



#### Data Protection Practices for ICT Systems

A robust and resilient infocomm technology system can help to protect against data breaches, thereby building trust in the organisation. Organisations can reference the framework provided in this **guide by PDPC to establish a governance structure** to determine and drive data protection policies and responsibilities, manage security risks by incorporating appropriate ICT controls and operationalise the policies by developing standard procedures and processes.



Scan here for  
more information



#### Data Breach Management Guide

Data breaches often lead to financial losses and loss of consumer trust for the organisation, hence it is important for organisations to proactively take steps to prevent, and if needed, to manage data breaches. This **guide by PDPC provides practical, actionable tips** on how to monitor risks and put in place a robust plan to manage data breaches. Detailed information on how the organisation should respond in the event of a data breach can also be found inside the guide.



Scan here for  
more information

## | Initiatives and Resources for Individuals

### Cybersecurity Labelling Scheme



The **Cybersecurity Labelling Scheme** (“CLS”) is a cybersecurity hygiene scheme for smart devices. Participating smart devices will be rated according to their levels of cybersecurity provisions. Consumers when shopping for smart devices should consider products that are rated under the scheme. This will enable consumers to identify products with better cybersecurity provisions and make informed decisions and for manufacturers with CLS-labelled products to gain a competitive advantage.



Scan here for  
more information

### Cyber Safety Activity Books And Interactive Handbook



CSA and PDPC developed a series of **Cyber Safety activity books** aimed at providing young readers with cyber tips to navigate cyberspace safely, as well as to raise awareness of the importance of cybersecurity and personal data protection.

In 2020, CSA also collaborated with SPF to develop an Interactive Handbook focusing on ways to spot online scams. These publications follow the **adventures of cyber defenders Crypto and Synthia**, in the style of a fun and interactive comic to educate children on cyber safety and inculcate good cyber hygiene habits from young.



Scan here for  
more information



### Scam Alert

Cybercrimes, particularly online scams, are on the rise and constantly evolving. The total number of scam cases reported increased by 65% from 2019 to 2020. Scams are usually designed to trick you into giving away your money, personal details or data by offering an attractive deal or false information. Top scams include social media impersonation and phishing scams. Individuals can learn how to spot the signs of scams and be updated on the latest scam trends in Singapore through **www.scamalert.sg**.



Scan here for  
more information

## Scamshield



'**ScamShield**,' a mobile application jointly developed by the Singapore Police Force and Government Technology Agency, and launched by the National Crime Prevention Council identifies and filters scam messages through the identification of key words using artificial intelligence. The application also blocks scam messages and phone numbers that were used in other scam cases or reported by other ScamShield users. This application is currently only available on iOS devices.



Scan here for  
more information

## Guide to understanding the PDPA for individuals



With the pervasiveness of technology, it is important to ensure your personal data will be safe with accountable organisations and used the way you want it to be. Always consider what data you should provide when transacting with an organisation and look out for organisations with the **Data Protection Trustmark**. Find out how else you can take steps to better protect your personal data with **Your Personal Data, Your Choice: A handy guide to understanding the PDPA for Individuals**.



Scan here for  
more information

## CONTACT INFORMATION



### To report a cyber incident

Email to [singcert@csa.gov.sg](mailto:singcert@csa.gov.sg) or access SingCERT's Cyber Incident Reporting form at <https://www.csa.gov.sg/singcert/reporting>



### To report a data breach

Submit a notification at <https://eservice.pdpc.gov.sg/case/db>, or call **+65 6377 3131** during work hours



### To seek scam-related advice

Anti-Scam hotline: **1800-722-6688**

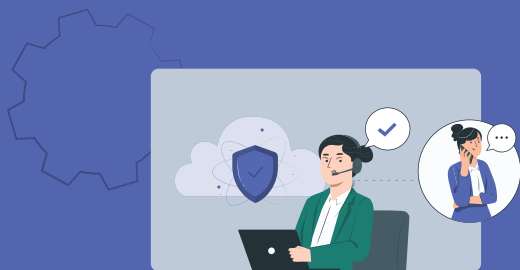
### To lodge a police report

Call **999** or SMS **71999**

Visit the **nearest Neighbourhood Police Centre/Post**

For police report that does not require immediate police action, please access the following website for lodging of electronic police report: <https://eservices.police.gov.sg>

**Do not hesitate to contact any of the three agencies when in doubt**



**CSA**



**SPF**



**PDPC**