
LEGAL ASPECTS OF INFORMATION SECURITY

IFS4101

WEEK 8, WELLY TANTONO, DIS, SOC, NUS

COMPUTER MISUSE ACT (CAP. 50)

LONG TITLE

“An Act to make provision for securing computer material against unauthorised access or modification, to require or authorize the taking of measures to ensure cybersecurity, and for matters related thereto.”

COMPUTER MISUSE ACT (CAP. 50)

SECTION NO.	SUBJECT MATTER
3	Unauthorised access to computer material
4	Access with intent to commit or facilitate commission of offence
5	Unauthorised modification of computer material
6	Unauthorised use or interception of computer service
7	Unauthorised obstruction of use of computer
8	Unauthorised disclosure of access code
9	Supplying, etc., personal information obtained in contravention of certain provisions
10	Obtaining, etc., items for use in certain offences
11	Enhanced punishment for offences involving protected computers
12	Abetments and attempts punishable as offences

CMA S 5: UNAUTHORISED MODIFICATION

Unauthorised modification of computer material

5.—(1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on conviction –

- (a) to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both; and
- (b) in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the act in question is not directed at —

- (a) any particular program or data;
- (b) a program or data of any kind; or
- (c) a program or data held in any particular computer.

(4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

WHAT DOES “UNAUTHORISED MODIFICATION” MEAN?

2 (7) For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer —

- (a) any program or data held in the computer concerned is altered or erased;
- (b) any program or data is added to its contents; or
- (c) any act occurs which impairs the normal operation of any computer,

and any act which contributes towards causing such a modification shall be regarded as causing it.

(8) Any modification referred to in subsection (7) is unauthorised if —

- (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and
- (b) he does not have consent to the modification from any person who is so entitled.

ELEMENTS OF “UNAUTHORISED MODIFICATION”

- What is the *mens rea*?
- What is the *actus reas*?
- How is “modification” defined?
- Is there any other form of harm / modification that we can think of that is not covered by the types of modification already defined in s 5?

WHAT IS SECTION 5 TRYING TO TARGET?

- Intended to deal with hackers who decide to modify systems after security access (e.g., system logs to cover tracks)
 - Hackers are almost invariably charged with unauthorised access (s 3) and unauthorised modification (s 5).
 - S 3 and s 5 are almost duplicative. Why have two of them? Is there any way that someone can be guilty of s 3 but not s 5?
- Also intended to deal with writers of viruses, Trojan horses, worms
 - Argument: “By writing the virus, I did not actually cause the computer to be modified or data to be deleted. It was the user who caused the computer to be infected.”
 - Rejected: “*any act which contributes towards causing such a modification shall be regarded as causing it*” – s 2(7), CMA

WHEN DOES UNAUTHORISED MODIFICATION TAKE PLACE?

- Is reflected (non-persistent) XSS “unauthorised modification”?
- Example of XSS at work - weather.com
- Question: Has anything been modified? Is the “modification” unauthorised?
- Three types of XSS

CMA S 6: UNAUTHORISED USE OR INTERCEPTION OF COMPUTER SERVICE

unauthorised use or interception of computer service

6.—(1) Subject to subsection (2), any person who knowingly

(a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any

 **computer service;**

(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an  **electromagnetic, acoustic, mechanical or other device;** or

(c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b),

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

CMA S 6: UNAUTHORISED USE OR INTERCEPTION OF COMPUTER SERVICE

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

(3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at

—

- (a) any particular program or data;
- (b) a program or data of any kind; or
- (c) a program or data held in any particular computer.

CMA S 6: UNAUTHORISED USE OR INTERCEPTION

- Derived from the Canadian Criminal Code, not the UK CMA
- How many activities are subject to criminalisation under Section 6?

THE STRAITS TIMES

Student reports hacking incidents.

By Chong Chee Kin.

503 words

29 April 1999

[Straits Times](#)

STIMES

English

(c) 1999 Singapore Press Holdings Limited

A NATIONAL University of Singapore law student has made a police report alleging that her computer account had been hacked into from an account with the Ministry of Home Affairs.

Ms Anne Lee, 21, told The Straits Times yesterday that her SingNet account was hacked into on 10 occasions over four days about two weeks ago.

A protection programme called Jammer, which she had installed in her computer, alerted her to the hacker. It gave her the Internet Protocol (IP) address of the hacker's computer as well as the dates and times of the hacker's intrusions.

According to a record of the hacker's activities shown to The Straits Times, the hacker had tried his luck at all hours of the day - even as early as 3 am. Once, he gained access to her computer three times in a single day.

"When I checked my computer, I was shocked to learn that someone using a program called Back Orifice had hacked into my system," she said.

"Although there did not seem to be any files missing, there was a lot of sensitive information in the computer, and I lost my things over the Internet."

ILLUSTRATION : SINGNET PORT SCANNING INCIDENT

ILLUSTRATION : **SINGNET PORT SCANNING INCIDENT**

- 29 April 1999: ST front page – NUS law student Anne Lee's SingNet account had been broken into on 10 occasions in 4 days
- Anne Lee installed Jammer software on her system
- Jammer recorded the IP address of the hacker's computer as well as dates and times of intrusions
 - According to a record of the hacker's activities shown to The Straits Times, the hacker had tried his luck at all hours of the day -even as early as 3 am. Once, the hacker gained access to her computer three times in a single day.
 - "When I checked my computer, I was shocked to learn that someone using a program called Back Orifice had hacked into my system," she said.
- Anne gave the IP address to SingTel Magix
- SingTel Magix told Anne that the account belonged to the Ministry of Home Affairs
- Anne Lee made police report on 20 April 1999

ILLUSTRATION : SINGNET PORT SCANNING INCIDENT

- 30 April 1999: ST front page – SingTel and SingNet admitted they had contracted with Ministry of Home Affairs' IT security unit to scan 200,000 SingTel/SingNet subscribers for security vulnerabilities
- SingTel CEO for Multimedia:
 - SingTel was being "responsible" by giving customers the "value-added service" of scanning their computers.
 - Asked if the law allowed it to do this without customers' consent, he said nothing illegal had taken place. *"We are merely protecting the interest of our customers."*
 - Customers were not informed of the scan, he said, so as not to alarm. *"We do not want to make a mountain out of a molehill. In the end, the scan might not turn up anything. If we had informed the customers, it might cause an alarm."*
 - He said MHA was approached as the ministry was the "expert" in this area - it had helped crack the case of the two teenage hackers.
- SingTel director Chang described the scan as *"a policeman patrolling in cyberspace checking if the 'windows' of the computer systems are opened"*.

ILLUSTRATION : SINGNET PORT SCANNING INCIDENT

- 30 April 1999: TAS – no laws were broken
 - “As far as TAS is concerned, there has been no violation of any TAS rules or regulations in this incident.... the IASPs may however want to consider keeping their customers informed in future.”
- 6 January 2000: IDA – Guidelines on Preventive Security Scanning
 - *“The government had stressed that such computer scanning without permission is wrong ...”*
 - *“The guidelines articulate the importance of accountability and transparency when security-conscious IASPs conduct scanning exercises to ensure that their subscribers' computers are safe and are not infected by malicious software or viruses. In particular, consent by IASP subscribers should be explicitly obtained before such exercises can be conducted. Scanning activities must be non-intrusive, and the IASP must inform its subscribers on how their privacy will be protected during such activities.”*

CMA S 7: UNAUTHORISED OBSTRUCTION OF USE OF COMPUTER

unauthorised obstruction of use of computer

7.—(1) Any person who, knowingly and without authority or lawful excuse —

- (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or
- (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer,

shall be guilty of an offence and shall be liable on conviction to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

(2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding \$50,000 or to imprisonment for a term not exceeding 7 years or to both.

 it is not possible to define out every attack that can be done since new attacks always arise

CMA S 7: UNAUTHORISED OBSTRUCTION'S PURPOSE

- Encrypting information making them inaccessible
- Denial of service ('DOS') attacks
 - CERT definition: "explicit attempt by attackers to prevent legitimate users of a service from using that service"
 - Examples:
 - Attempts to flood a network
 - Attempts to disrupt connections between two machines
 - Attempts to prevent a particular individual from accessing a service
 - Attempts to disrupt service to a specific system or person
 - Modes of attack
 - Consumption of scarce, limited or non-renewable resources such as memory and disk space, CPU time, network bandwidth (e.g., ping of death attacks)
 - Destruction or alteration of configuration information (e.g., router information)
 - Physical destruction or alteration of network components
 - From one machine or from many machines (distributed denial of service ('DDOS') attacks)

CMA S 7: UNAUTHORIZED OBSTRUCTION OF USE

PPV KENDRICK TAN (2000) (SUBORDINATE COURTS - NO JUDGMENT)

- Kendrick Tan (MBA graduate) and wife put in an application to HDB for purchase of resale flat
- Transaction delayed due to delay by HDB in processing Tan's application
- Tan's wife sent email reminder to HDB
- On 31 December 1999, Tan sent 2,500 email in 2 1/2 hours to 3 separate and different HDB mailboxes, enclosing wife's email, seeking response
- DPP: "What Tan did was an offence under the CMA as he had sent an enormous amount of email to HDB's mailbox, which could have crashed as a result"
- Fined \$30,000 - cost: \$4 per email

 this shows that s7 is used not just for DDOS but also for other attacks which can include unreasonable spamming

how to take be guilty in section 3 but without section 5

LOCAL CYBERCRIME

- Tan Hian Chye placed 1,908 false bids on eBay worth US\$6 million (for items valued at US\$2 million) to disrupt activities of more than 1000 sellers in Feb and March 2002
- Tan fined \$27,000 - \$9,000 each on **3 charges** under the Computer Misuse Act – for disrupting the bidding process
- Quaere: Is this a CMA, s 7 case on **“unauthorised obstructions”**?

THE STRAITS TIMES

Man disrupted Net auctions with \$10m bogus bids.

By Selina Lum.

592 words

14 April 2004

[Straits Times](#)

STIMES

English

(c) 2004 Singapore Press Holdings Limited

He hindered bidding on eBay site by making 1,908 bids for items he did not intend to buy. He is fined \$27,000 on three charges

IN JUST a month, a Singapore man made successful bids totalling US\$6 million (S\$10 million) with online auction site eBay for items valued at about US\$2 million - but he had no intention of buying anything.

Using 10 of the 86 accounts he created with the site, Tan Hian Chye, 42, placed 1,908 false bids to disrupt the activities of more than 1,000 sellers in February and March 2002.

He then ended the auctions by either making high bids or by pretending to buy the item at the price specified by the seller.

eBay, based in San Jose, California, received about 1,500 e-mail messages from 1,073 sellers complaining about the 10 accounts created by Tan, who was then a Singapore Armed Forces regular.

Although no damage was caused to its computer servers, the company spent about US\$39,000 in man-hours responding to the complaints and looking into the disruptions.

Yesterday, a district court here fined Tan a total of \$27,000 - \$9,000 each on three charges under the Computer

CMA S 8: UNAUTHORISED DISCLOSURE OF ACCESS CODE

Unauthorised disclosure of access code

8.—(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any computer shall be guilty of an offence if he did so —

- (a) for any wrongful gain;
- (b) for any unlawful purpose; or
- (c) knowing that it is likely to cause wrongful loss to any person.

(2) Any person guilty of an offence under subsection (1) shall be liable on conviction —

- (a) to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both; and,
- (b) in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

- What's the legislative objective behind this provision?
- Was it necessary to introduce this as a crime? If not, why and if yes, why? Could this have been addressed through other provisions?

CMA S 8: UNAUTHORISED DISCLOSURE OF ACCESS CODE


- Reading the CMA as it stood at 1998, what was wrong with S 8?
- What types of harms did it fail to address? Put it another way, if you had nefarious intent, what could you have done to cause harm and still not get into trouble given where the CMA stood in 1998?

intent will be very difficult to prove - and the pentesting companies should be clear that tools are only used within their own company licensed work

CMA S 10: OBTAINING, ETC., ITEMS FOR USE IN CERTAIN OFFENCES

Obtaining, etc., items for use in certain offences

10.—(1) A person shall be guilty of an offence if the person —

- (a) obtains or retains any item to which this section applies —
 - (i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or
 - (ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or
- (b)  makes, supplies, offers to supply or makes available, by any means any item to which this section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7.

(2) This section applies to the following items:

- (a) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7;
- (b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed.

CMA S 10: OBTAINING, ETC., ITEMS FOR USE IN CERTAIN OFFENCES

con't

- (3) A person guilty of an offence under subsection (1) shall be liable on conviction —
- (a) to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both; and
 - (b) in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.

COMPARISON WITH S 3A OF THE UK CMA

3A Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA

- (1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
- (2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
- (3) A person is guilty of an offence if he obtains any article—
 - (a) intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or
 - (b) with a view to its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.
- (4) In this section “ article ” includes any program or data held in electronic form.
- (5) ...

CMA S 9: PARLIAMENTARY DEBATES 2017

- "To ensure that the provision does not inadvertently prohibit legitimate access by cybersecurity professionals to such tools, this is an offence only if the act is carried out with the intention of committing or facilitating the commission of a computer crime."
- delimiter is *mens rea*
 - but how to construe "with a view to its being supplied [or made available]"? lower or higher threshold?
 - Minister overstated the *mens rea*, which has a much lower threshold
 - e.g. X supplied port scanners or keystroke loggers, not intending or facilitating the commission of a s 6(1)(b) offence, but certainly "has a view" that its supply may assist in the commission of an offence!

CMA S 9: SUPPLYING, ETC., PERSONAL INFORMATION OBTAINED IN CONTRAVENTION OF CERTAIN PROVISIONS

Supplying, etc., personal information obtained in contravention of certain provisions

9.—(1) A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 —



obtains or retains the personal information; or

(b)

supplies, offers to supply, transmits or makes available, by any means the personal information.

- (2) It is not an offence under subsection (1)(a) if the person obtained or retained the personal information for a purpose other than —
- (a) for use in committing, or in facilitating the commission of, any offence under any written law; or
 - (b) for supply, transmission or making available by any means for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law.
- (3) It is not an offence under subsection (1)(b) if —
- (a) the person did the act for a purpose other than for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law; and
 - (b) the person did not know or have reason to believe that the personal information will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law.

CMA S 9: SUPPLYING, ETC., PERSONAL INFORMATION OBTAINED IN CONTRAVENTION OF CERTAIN PROVISIONS

- (4) For the purposes of subsection (1)(b), a person does not transmit or make available personal information merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data.
- (5) A person guilty of an offence under subsection (1) shall be liable on conviction —
- (a) to a fine not exceeding \$10,000 or to imprisonment for a term not exceeding 3 years or to both; and
 - (b) in the case of a second or subsequent conviction, to a fine not exceeding \$20,000 or to imprisonment for a term not exceeding 5 years or to both.
- (6) For the purpose of proving under subsection (1) that a person knows or has reason to believe that any personal information was obtained by an act done in contravention of section 3, 4, 5 or 6, it is not necessary for the prosecution to prove the particulars of the contravention, such as who carried out the contravention and when it took place.

COMPARE DEFINITION OF PERSONAL INFORMATION IN CMA WITH PERSONAL DATA IN PDPA

- CMA S. 9(7)
- (7) In this section —
 - (a) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and
 - (b) a reference to an offence under any written law includes an offence under subsection (1).

S 9 CMA: ANALYSIS OF PARLIAMENTARY DEBATES, 2017

- "The new section [9], therefore, closes the gap by making it an offence to obtain or deal in such personal information. The new section [9] criminalises acts done in relation to personal information of individuals that the perpetrator knows or has reason to believe had been obtained by committing a computer crime. The act of obtaining or retaining such personal information will be an offence; as will be supplying, offering to supply, transmitting or making available that information.
- It is not the Government's intent to criminalise legitimate cybersecurity industry practices. We understand that cybersecurity professionals may deal with hacked personal information in the course of their work. For instance, they may transmit such information for the purpose of analysing a data breach, or for the purpose of highlighting vulnerabilities in a system.
- We have, therefore, introduced exceptions in section [9]. It is not an offence if the individual obtained or retained the personal information for a legitimate purpose. It is also not an offence if the individual supplied, offered to supply, transmitted or made available the personal information for a legitimate purpose, and they did not know or have reason to believe that the information will be or is likely to be used to commit an offence."
- Senior Minister of State for Home Affairs, Desmond Lee, 2nd Reading

S 9: ELEMENTS OF THE CRIME

- **actus reus:**

- person obtains, retains, supplies, offers to supply, transmits, makes available, by any means, "personal information"

- **mens rea:**

- knows or has reason to believe that the "personal information" about another person (being an individual) was obtained by an act done in [breach of CMA]
- not necessary (for prosecution) to prove "particulars of contravention [/breach]" of CMA such as "who carried out the contravention and when it took place"

S 9: ELEMENTS OF THE CRIME: DEFINITION OF PERSONAL INFORMATION

- What is "personal information"?
 - now both a CMA issue and a PDPA issue
 - can personal data not be protected under PDPA but protected under CMA (and vice versa)?

COMPARE DEFINITION OF PERSONAL INFORMATION IN CMA WITH PERSONAL DATA IN PDPA

CMA S. 9(7)

(7) In this section —

- (a) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and
- (b) a reference to an offence under any written law includes an offence under subsection (1).

PDPA S. 2

“personal data” means data, whether true or not, about an individual who can be identified —

- (a) from that data; or
- (b) from that data and other information to which the organisation has or is likely to have access;

S 8A: ELEMENTS OF THE CRIME: DEFINITION OF PERSONAL INFORMATION

- What is "personal information"?
 - now both a CMA issue and a PDPA issue
 - can personal data not be protected under PDPA but protected under CMA (and vice versa)?
- Must "personal information" be "illicit"?
- prosecution does not need to prove that "personal information" was [illicit], or that "details '[such as ... who ... and when]'" so how would defendant "know or have reason to believe" that information is "illicit"?
- some information is obviously "illicit" e.g. marked as such, credit card numbers
- not so obvious for other information e.g. addresses, email addresses (what if gathered legitimately)

S 9: ELEMENTS OF THE CRIME: NATURE OF THE OFFENCE

- NOT criminalization of commercial dealings in "illicit personal information", but...
- Obtaining, retaining, [dealing] [see the Parliamentary Debates] in "personal information" which prosecution need not definitely prove is "illicit"
- Note Subsections (2) and (3) which shift the burden of proof from the prosecutor to defendant. It is now defendant's burden to show obtaining, retaining or dealing in personal information "for a purpose other than (a) for use in committing ... any offence under any written law" and defendant did not know or has reason to believe personal information "will be or is likely to be used to commit ... any offence under any written law" [note: conjunctive "or"!]
- **Question:**
- **The burden of proof of which elements of the crime are being shifted by Subsections (2) and (3)?**

S. 9 PARLIAMENTARY DEBATES

"Ultimately, we need to strike a balance between protecting the public interest, and ensuring that legitimate practices of the cybersecurity industry can continue. It would not be difficult for bona fide cybersecurity professionals to explain why they have hacked personal information in their possession. It is also not the Police's intention to demand that every cybersecurity professional provide such explanations. Rather, in the course of investigations into a CMCA offence, Police need to have the powers to deal with individuals who are found to have such personal information belonging to others.

Fundamentally, care should be exercised when dealing with personal information, especially information that has been hacked and may be subsequently used in the commission of an offence. This applies also to cybersecurity professionals. ...

Care should always be exercised where hacked personal information is transmitted, even if for a legitimate purpose. This could be done by ensuring that the information is only transmitted to trusted persons who have a legitimate reason to receive the information. Where possible, the personal information should be redacted or anonymised."

Senior Minister of State for Home Affairs, Desmond Lee, 2nd Reading

THE DIFFICULTY WITH DAMAGES


DAMAGE & ENHANCED PENALTIES

ENHANCED PENALTIES: S 3(2) (HACKING), S 5(2) (MODIFICATION), S 6(2) (USE/INTERCEPTION), S 7(2) (OBSTRUCTION)

- CMA s 2 Interpretation.
 - “damage” means, except for the purposes of section 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that —
 - (a) causes loss aggregating at least \$10,000 in value, or such other amount as the Minister may, by notification in the *Gazette*, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account;
 - (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons;
 - (c) causes or threatens physical injury or death to any person; or
 - (d) threatens public health or public safety;

DAMAGE & ENHANCED PENALTIES

ENHANCED PENALTIES: S 3(2) (HACKING), S 5(2) (MODIFICATION), S 6(2) (USE/INTERCEPTION), S 7(2) (OBSTRUCTION)

-  How should we conceptualise damages in cyberspace?
- What is the difference between “damage” from cyberattacks in the electronic environment and “damage” as defined in the CMA?
- As a cybersecurity professional, what type of events would you deem to be damage and is that damage addressed by the CMA’s definition of the term “damage”?
- What is the general effect of showing damage that is caused from a cyberattack under one of the CMA provisions?

WHAT DO DAMAGES LOOK LIKE IN CYBERSPACE?

- Concept of "damages" in an electronic environment
 - few real world analogies
 - "damage" is loss, harm or deterioration caused to another, deprivation of or interference with possession or use
- cf: reversibility of "damage" in many electronic contexts makes electronic "damage" more of an inconvenience, especially if changes can be reinstated expeditiously
 - CMA side-steps problem of "damage" for basic offences
 - But "damage" (as statutorily defined) triggers enhanced penalties for each basic offence

HOW DO WE QUANTIFY DAMAGES IN AN ELECTRONIC ENVIRONMENT?

- What does loss aggregating at least \$10,000 in value mean?
 - What about cost of security evaluation and assessment?
 - If data is worth \$1 million and it costs \$1,000 to restore it, is it a loss of \$1 million or a loss of \$1,000?
 - The data is worth \$5,000 but because the data loss alerts you to the lack of security in the company, you conduct a very thorough clean-up action to patch up all of the vulnerabilities and that exercise costs the company \$50,000. Does that \$50,000 represent the loss that is covered under the CMA?
 - What about (unmonetizable or hardly monetizable) time and effort expended to restore the data?
 - Is inconvenience quantifiable?
 - As a result of the DDOS attack, the social media platform was suspended for 5 hours. However, this is a new company and frankly, not too many ads are being served because it's at an incubation phase. However, as a result of the user's frustration with login, many decided to move to the competitor's platform. The company is loss-making and charges users nothing and is running aggressive promotion such that ad spots are effectively free. How do you quantify the loss?
 - What is the platform's technology was awful to begin with and, frankly, has been losing users at a rate that's been accelerating for the last 6 months?
 - What if the DDOS attack was launched by the competitor, who found out that the company was about to overhaul the platform with a competitor killer technology 6 hours before they launched the DDOS?

SS 16 AND 17 CMA: COMPOSITION OF OFFENCES AND COMPENSATION

- S 16
 - Provides for the composition of offences – effectively a “plea bargain” and the accused will be fully acquitted.
 - The Minister may make regulations to prescribe the offences which may be compounded.
 - Does not apply to enhanced penalties.
- S 17
 - Court is empowered to order the accused to compensate the victim for damage caused
 - Compensation is independent of separate redress in civil proceedings

S 12 CMA: ABETMENTS AND ATTEMPTS PUNISHABLE AS OFFENCES

Abetments and attempts punishable as offences

12.-(1) Any person who abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) For an offence to be committed under this section, it is immaterial where the act in question took place.

- Cyberattack abetments/ attempts treated as full offences
- Rationale: to discourage preparations towards and joint participations in cyberattack activities

WHAT IS AN ABETMENT?

- “Secondary participation: – where secondary offender (abettor) incurs liability of primary perpetrator
- Secondary liability arises from assistance or encouragement of offence, or participation in criminal enterprise
- Examples: instigation, criminal conspiracy, intentionally aiding (by act or illegal omission) of doing of [offence]
- Abettor's liability founded on combination of guilty *mens rea* with (hypothetical) actus reus
- For an offence to be committed under this section, it is immaterial where the act in question took place.

DEFINITION OF ABETMENT (S. 107 OF THE PENAL CODE)

Abetment of the doing of a thing

107.—(1) A person abets the doing of a thing who —

- (a) instigates any person to do that thing;
 - (b) engages with one or more other person or persons in any conspiracy for the doing of that thing, if an act or illegal omission takes place in pursuance of that conspiracy, and in order to the doing of that thing; or
 - (c) intentionally aids, by any act or illegal omission, the doing of that thing.
- (2) A person may abet the doing of a thing despite the existence of facts of which he is unaware which make the doing of the thing impossible.

Explanation 1.—A person who, by intentional misrepresentation, or by intentional concealment of a material fact which he is bound to disclose, voluntarily causes or procures, or attempts to cause or procure, a thing to be done, is said to instigate the doing of that thing.

Illustration

A, a public officer, is authorised by a warrant from a court of justice to apprehend Z. B, knowing that fact and also that C is not Z, intentionally represents to A that C is Z, and thereby intentionally causes A to apprehend C. Here B abets by instigation the apprehension of C.

Explanation 2.—Whoever, either prior to or at the time of the commission of an act, does anything in order to facilitate the commission of that act, and thereby facilitates the commission thereof, is said to aid the doing of that act.

the crime is completed even when in the below scenarios

: mens rea of the abettor + actus rea of the person who is of unsound mind

DEFINITION OF ABETMENT (S. 108 OF THE PENAL CODE)

108. A person abets an offence who abets either the commission of an offence, or the commission of an act which would be an offence, if committed by a person capable by law of committing an offence with the same intention or knowledge as that of the abettor. ...

- Explanation 3.—It is not necessary that the person abetted should be capable by law of committing an offence, or that he should have the same guilty intention or knowledge as that of the abettor, or any guilty intention or knowledge.
- Illustrations [Innocent Agent]
 - (a) A, with a guilty intention, abets a child or a person of unsound mind to commit an act which would be an offence if committed by a person capable by law of committing an offence, and having the same intention as A. Here A, whether the act is committed or not, is guilty of abetting an offence.
 - (b) A, with the intention of murdering Z, instigates B, a child under 7 years of age, to do an act which causes Z's death. B, in consequence of the abetment, does the act, and thereby causes Z's death. Here, though B was not capable by law of committing an offence, A is liable to be punished in the same manner as if B had been capable by law of committing an offence and had committed murder, and he is therefore subject to the punishment of death.
 - (c) A instigates B to set fire to a dwelling-house. B, in consequence of the unsoundness of his mind, being incapable of knowing the nature of the act, or that he is doing what is wrong or contrary to law, sets fire to the house in consequence of A's instigation. B has committed no offence, but A is guilty of abetting the offence of setting fire to a dwelling-house, and is liable to the punishment provided for that offence.
 - (d) A, intending to cause a theft to be committed, instigates B to take property belonging to Z out of Z's possession. A induces B to believe that the property belongs to A. B takes the property out of Z's possession, in good faith believing it to be A's property. B, acting under this misconception, does not take dishonestly, and therefore does not commit theft. But A is guilty of abetting theft, and is liable to the same punishment as if B had committed theft.


DEFINITION OF ABETMENT (S. 108 OF THE PENAL CODE)

Explanation 5.—It is not necessary to the commission of the offence of abetment by conspiracy that the abettor should concert the offence with the person who commits it. It is sufficient if he engages in the conspiracy in pursuance of which the offence is committed.

Illustration

A conspires with B a plan for poisoning Z. It is agreed that A shall administer the poison. B then explains the plan to C, mentioning that a third person is to administer the poison, but without mentioning A's name. C agrees to procure the poison, and procures and delivers it to B for the purpose of its being used in the manner explained. A administers the poison; Z dies in consequence. Here, though A and C have not conspired together, yet C has been engaged in the conspiracy in pursuance of which Z has been murdered. C has therefore committed the offence defined in this section, and is liable to the punishment for murder.

EXAMPLES OF ABETMENTS

- Some examples (adapted from s 108, Penal Code illustrations) (A2 is abettor, A1 is primary perpetrator, V is victim)
- A2 instigates A1 to hack V's computer. A1 refuses. A2 is guilty of abetting A1 of “unauthorized access”.
-  A2, intending to access to V's system, tricks A1 into telling V to set her password to “reset” because of a company-wide system reset requires all passwords to be “reset”. A2 is guilty of abetting the offence of “unauthorised disclosure of access code” in s 8, CMA (“innocent agent” doctrine).

S 12 CMA: WHAT IS AN ATTEMPT?

- "Inchoate offences"
 - where the commission of an offence has just begun, including any act preparatory to or in furtherance of the commission of any offence, or
 - where the crime failed
- Section 511 of the Penal Code:
 - (1) A person attempts to commit an offence punishable by this Code or by any other written law who, with the intention of committing that offence takes a **substantial step towards the commission of that offence**.
 - (2) For the purposes of subsection (1), an act is a substantial step towards the commission of an offence if it is **strongly corroborative of an intention to commit the offence** ...
 - (3) A person may attempt the doing of a thing despite the existence of facts of which he is unaware which make the doing of the thing impossible.

GROUP DISCUSSION TIME : ATTEMPTED MURDER OF A CORPSE

-
- Discuss the following scenario:
 - At 4:00 p.m. John goes to his study for his afternoon nap, as is his wont, lies down, and dies in his sleep at 4:10 p.m. At precisely 4:30 p.m. Alice sneaks into John's study, thinking he is asleep on the couch and stabs him thirteen times in the chest. Clearly, Alice hasn't murdered John since he was already dead. But is she guilty of attempted murder?

*(courtesy of Teuber from
<http://people.brandeis.edu/~teuber/puzz12.html>)*

S 12 CMA: WHAT IS AN ATTEMPT?

- Examples from Section 511 of the Penal Code
 - (a) A makes an attempt to steal some jewels by breaking open a box, and finds after so opening the box that there is no jewel in it. He has done an act towards the commission of theft, and therefore is guilty under this section.
 - (b) A makes an attempt to pick the pocket of Z by thrusting his hand into Z's pocket. A fails in the attempt in consequence of Z's having nothing in his pocket. A is guilty under this section.
- Example adapted from Section 511
 - A tried to gain unauthorized access to V's computer system. He first tried the default company password. It did not work. He next tried "password" as the password. It also did not work. A was caught by his manager. A has committed the offence of "attempted unauthorized access".

S 12 CMA: ABETMENTS AND ATTEMPTS PUNISHABLE AS OFFENCES

- In the context of s 12, CMA, is it any “act preparatory to or in furtherance of the commission of any offence” that would trigger criminal sanction? How should this element of the offence be interpreted? For instance, consider the following scenarios:
 - Alan wanted to hack into Vivian’s computer system. He found a post-it with what looks like Vivian’s password stuck to Vivian’s computer monitor. He used that and tried to log in. It did not work.
 - As above, and Alan had just started up Vivian’s computer but before he could log on, when Vivian appeared and said, “What are you doing here?”

IF we change the scenario to become:

Alan saw the post-it and starts up the computer - then Vivian immediately comes and asks him what he is doing

this is now much less clear


not all systems that belong to mindef will fall under this - there is a need to have both actus rea and mens rea

S 11 CMA: ENHANCED PUNISHMENT FOR OFFENCES INVOLVING PROTECTED COMPUTERS

Enhanced punishment for offences involving protected computers

11.—(1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable to a fine not exceeding \$100,000 or to imprisonment for a term not exceeding 20 years or to both.

(2) For the purposes of subsection (1), a computer shall be treated as a “protected computer” if the person committing the offence **knew, or ought reasonably to have known**, that the computer or program or data is used directly in connection with or necessary for —

-  **the security, defence or international relations of Singapore;**
- (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;**
- (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or**
- (d) the protection** of public safety including systems related to essential emergency services such as police, civil defence and medical services.

(3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised access to that computer, program or data attracts an enhanced penalty under this section.

GROUP DISCUSSION TIME: REAL LIFE CASE - WHAT CRIMES CAN BE CHARGED?

-
- Tan Chye Guan Charles v PP [2009] 4 SLR(R) 5
 - **Facts:** In early 2007, DSTA invited bids from various suppliers to tender for a contract to build a munitions container storage system for the SAF. Before submitting his company's bid, CT met with the MINDEF project manager. During that meeting, the project manager stepped away from his laptop. CT saw some information submitted by other suppliers to DSTA which could help him gain competitive advantage in the bid. He inserted a thumb drive into the laptop and copied the file. DSTA admitted that the information copied by CT was commercial in nature.
 - Has CT committed a s 3 + s 11 (protected computers) offence?

in this case, phishing to get the password for unauthorised access would fall under CMA
 - but phishing and scamming victims into sending them money will not fall under CMA
 (since the victim willingly and has the authority to send)

OTHER OFFENCES THAT MAY BE CYBER-RELATED BUT NOT COVERED BY CMA

Nature of Offence	Legislation	Section
Theft of funds, economic losses	Penal Code	S 378 (theft) S 383 (extortion) S 403 (criminal misappropriation of property) S 405 (criminal breach of trust)
Personal harm or injury	Penal Code	S 319 (hurt) S 376E (sexual grooming) S 503 (criminal intimidation) S 590 (outraging modesty)
Privacy and data protection	PDPA	S 51 (offences)
Disturbing social order	Penal Code Sedition Act	S 298 (words wounding religious/racial feelings) S 298A (promoting enmity on grounds of religion/race or prejudicial to maintenance of harmony) S 4 (offences)
Copyright infringement	Copyright Act	S 136 (offences for commercial dealings) S 260 (removal of rights management information offences) S 261C (circumvention of technological measures offences)

OTHER OFFENCES THAT MAY BE CYBER-RELATED BUT NOT COVERED BY CMA

Nature of Offence	Legislation	Section
Doxing, stalking, harassment	Protection from harassment act	S 3 (intentional harassment, alarm or distress including through doxing) S 4 (harassment, alarm or distress including through doxing – note lower intent) S 5 (fear, provocation or facilitation of violence) S 6 (offences against public servant) S 7 (stalking including cyber)
Failure to take down fake news	Protection from online falsehoods and manipulation	S 8 (bots propagating falsehoods) S 36 (operating banned sites) S 37 (failure to take down information) S 42 (failure to block accounts)

SUMMARY OF ATTACKS AGAINST COMPUTING RESOURCES

Hacking	Unauthorised access to programs and data – s 3 With intent to commit offence – s 4
Trojan, worms, virus attacks	Unauthorised modification – s 5, CMA
Collecting user-IDs, passwords via trapdoors, spyware, spoofing, intercepting communications	Unauthorised interception – s 6, CMA
Denial of service ('DOS') attacks , distributed DOS	Unauthorised obstruction of use of computer – s 7, CMA
Sale or trade in passwords or means of gaining access	Unauthorised disclosure of access codes – s 8, CMA
Attacks against infrastructure computers	Protected computers – s 11, CMA
Cyberattack attempts	Abetments and attempts – s 12, CMA

MODALITIES PROBLEM: IN A GLOBAL WORLD, HOW WOULD NATION STATES REGULATE AGAINST TRANS-BORDER CRIMES?

Territorial scope of offences under this Act

13.—(1) Subject to subsection (3), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore.

(2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore.

(3) For the purposes of this section, this Act applies if —

- (a) for the offence in question, the accused was in Singapore at the material time;
- (b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time; or
- (c) **the offence causes, or creates a significant risk of, serious harm in Singapore.**

S 13 CMA: TERRITORIAL SCOPE

In subsection (3)(c), “serious harm in Singapore” means —

- (a) illness, injury or death of individuals in Singapore;
- (b) a disruption of, or a serious diminution of public confidence in, the provision of any essential service in Singapore;
- (c) a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or
- (d) damage to the national security, defence or foreign relations of Singapore.

S 13 CMA: TERRITORIAL SCOPE

Example 1.—The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:

- (a) publication to the public of the medical records of patients of a hospital in Singapore;*
- (b) providing to the public access to the account numbers of customers of a bank in Singapore.*

Example 2.—The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board:

- (a) providing to the public access to confidential documents belonging to a ministry of the Government;*
- (b) publication to the public of the access codes for a computer belonging to a statutory board*

S 13 CMA: TERRITORIAL SCOPE

Accused's Location	Victim's Location	Computer / Data's Location	CMA applies?
Singapore	??	Not in Singapore	Yes – S 13(3)(a)
Not in Singapore	??	Computer, program or data physically in Singapore at the material time	Yes – S 13 (3)(b)
??	Singapore's interests suffer "serious harm" or individual victim suffers illness, injury or death	??	Yes – S 13(3)(c)

IN CONCLUSION

- Computer Misuse Act (Computer Misuse and Cybersecurity Act) drafted with computer-related offences in mind
- Provisions are extremely wide and all-embracing, and cover a wide range of cyberattacks
 - Hacking/aggravated hacking: ss 3, 4
 - Modification: s 5
 - Use/interception: s 6
 - Obstruction: s 7
 - Password laundering: s 8
 - Dealings with personal data: s 9
 - Dealings with tools for hacking: s 10
 - Protected computers: s 11
 - Attempts/abetment: s 10

IN CONCLUSION

- Breadth of substantive offences vs. lack of precision with some elements, particularly "authorisation"
- Multiple offences may fit one cybercrime activity
- Some uncertainty about scope of cybercrime offences e.g. ss 4, 6
- "Data-oriented" and "tool-oriented" offences in ss 8, 9, 10 are very broad and even more uncertain
- Room for dispute and management of risk exposure by corporations and institutions