
Computer
Crime

Learning Objectives

- Describe the Computer Misuse Act Chpt 50A (“CMA”)
- Understand the various interpretations in the CMA
- Evaluate the offences and penalties under the CMA
- Describe the territorial scope of the CMA
- Evaluate the mitigating factors for criminal offences

Background

Why is there a need for a Computer Misuse Act and a Cybersecurity Act in Singapore?

- An “Intelligent Island”, A “Financial Hub”, “ Smart Nation”
- Information Technology has become very pervasive in every aspect of society (government, business, households)
- Rising crime rate relating to the use of computers (in 2018, there were 1024 cases reported under the Computer Misuse Act, increase of 40% compared to 2017)
- There were 6,179 cybercrimes in 2018, up from 5,351 in 2017

Objectives of Computer Misuse Act

- Enhance security in areas like financial transactions, defence, telecommunication, public utilities, airport control, road traffic light control system.
- Deterrence – punishment to be commensurate with severity of offence (making unattractive to commit the offence)

"Cyber crimes not only undermine public and international confidence in the commercial integrity and viability of our computer systems, it also gravely compromises Singapore's efforts to position itself as a global e-commence hub. The potential for which these cyber crimes have in undermining Singapore's burgeoning IT industry cannot be ignored. IT security is a major consideration when investors decide to invest in the local IT sector"

- *PP v. Muhd Nuzaihan,* Chief Justice Yong Pung How, 2000

Cybersecurity Act (Act 9 of 2018)

- On 5 February 2018, Parliament passed the **Cybersecurity Act (Act 9 of 2018)** to take measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure (CII), to regulate cybersecurity service providers. The Act came into force on 31 August 2018.

- "Cybersecurity": the state in which a computer or computer system is protected from unauthorised access or attack. An example of a cybersecurity threat is a phishing email, or an email that is infected with a malicious computer program. A cybersecurity incident is essentially a cybersecurity threat that has been realised. Hence, the accessing of a hyperlink in a phishing email by the recipient resulting in the installation of a malicious computer program on the recipient's computer.

- Comprehensive cybersecurity law that covers standard setting, information sharing and incident management.

- The CII are computer systems directly involved in provision of essential services and the CII sectors are Energy, Water, Banking and Finance, Healthcare, Transport (which includes Land, Maritime, and Aviation), Infocomm, Media, Security and Emergency Services and Government.

https://www.csa.gov.sg/legislation/cybersecurity-act

Cybersecurity Act (Act 9 of 2018)

- The Act provides a framework for the designation of CII, and provides CII owners with clarity on their obligations to proactively protect the CII from cyber-attacks e.g. CII owner is required to notify Cyber Security Agency of Singapore (CSA) of change in ownership, as well as conduct audits and cybersecurity risk assessment. Non-compliance without reasonable excuse is a criminal offence which attracts a fine and/or imprisonment.

- The Act also authorizes CSA to prevent, investigate and respond to cybersecurity threats and incidents (based on level of severity). And CSA can request cybersecurity information – as information sharing / timely information is critical to help the government and owners of computer systems identify vulnerabilities and prevent cyber incidents more effectively.

- In addition, the Act establishes a licensing framework (yet to be implemented) for cybersecurity service providers whereby CSA will currently license 2 types of service providers, namely penetration testing and managed security operations centre (SOC) monitoring. Providers of such services have access to sensitive information from their clients. They are also relatively mainstream in our market and hence have a significant impact on the overall security landscape. CSA will continue to monitor international and industry trends and assess if new types of cybersecurity services are considered high-risk, and evaluate whether the providers of such services should be licensed

CMA, on the other hand, mainly deals with cybercrimes such as the unauthorised access of computer material, does not provide a regulatory framework for the routine and proactive protection of CII.

CMA vs CA 2018

- NOTE: **Computer Misuse Act and Cybersecurity Act are complementary**.

- **Computer Misuse Act:** investigation and prosecution of computer crimes

- **Cybersecurity Act:** protect computer systems in Singapore, especially CII, against cybersecurity threats and incidents.

Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

ng Prime Minister Lee Hsien Loong and a few ministers, have had their personal data
had their outpatient prescriptions stolen.

Computer Misuse Act (CMA) Interpretation

Interpretation *(excerpts)*

2. —(1) In this Act, unless the context otherwise requires —

"computer" "computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, 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 or group of such interconnected or related devices, but does not include — (a) an automated typewriter or typesetter; (b) a portable hand-held calculator; (c) a similar device which is non-programmable or which does not contain any data storage facility; or (d) such other device as the Minister may, by notification in the Gazette, prescribe;

"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;

Computer Misuse in Action (video)

https://video.search.yahoo.com/search/video;_ylt=Awr9H6q6ONJd7IQAihZXNyoA;_ylu=X3oDMTEyY3NpdDQ1BGNvbG8DZ3ExBHBvcwMxBHZ0aWQDQjkwMTNfMQRzZWMDc2M-?p=crimewatch+2018+episode+8&fr=mcafee#id=4&vid=5d610eb70cae4d8e06f63215ea8f20d6&action=view

Computer Misuse Act (CMA)

OFFENCES

- Section 3 – Hacking & securing access without authority
- Section 4 – Using a computer to commit an offence (fraud, dishonesty, property, bodily harm)
- Section 5 – Unauthorised modification of computer contents
- Section 6 – Unauthorised use of computer services
- Section 7 – interference, interruption, obstruction, impeding access and/or impairing effectiveness of a computer (also encompass “email bombing” and “spam”)
- Section 8 – Unauthorised disclosure of Password
- Section 8A – Dealing in hacked personal information
- Section 8B – Dealing in hacking tools
- Section 9 – “Protected” Computers
- Section 10 – Abetments

Section 3 - Unauthorised Access to Computer Material

Unauthorised access to computer material

- **3.** —(1) Subject to subsection (2), any person who **knowingly causes a computer to perform any function** for the purpose of **securing access without authority** to any program or data held in any computer shall be guilty of an offence

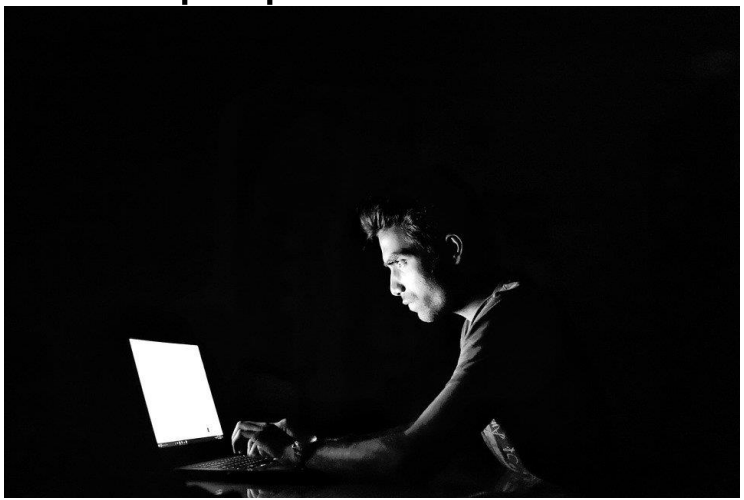
- First offence punishment: fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both
- Subsequent offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.
- If damage is caused: fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.
- Appropriate sentence depends on kind of program or data accessed; the level of sophistication in securing the access; the stage of access secured; the ease or difficulty of the detection; the extent of damage (if any); the potential for mischief caused by the illicit entry; and the degree of persistency in offending

Section 3 - Unauthorised Access to Computer Material

- Section 3 deals with unauthorised access to browse through other computer user's computers. No need malicious intent e.g. could be just to show how insecure certain websites are. Access need not be to a particular 'targeted' computer – hackers frequently dial randomly in attempt to discover IP addresses and telephone numbers which will provide contact with a computer system. Phishing activities.
- Section 3 also deals with users who exceed their authority and access parts of a system officially denied to them e.g. employees keen to access and download company's confidential information.

Lim Siong Khee v PP (2001)

- Lim and Ms Chong were a couple.
- In April 1999, Ms Chong ended their relationship after going on a trip to Europe with Lim.
- Ms Chong subsequently encountered problems accessing her email and suspected that Lim has tampered with her email account.
- Lim had guessed her account password and had gone to circulate an email titled “Special Relation” to three of Ms Chong’s friends.
- The email contained lurid details of her purported “relations” with Lim during their Europe trip.



Judgment

- Lim was convicted after trial on a charge of knowingly causing an email server to perform a function for the purpose of securing unauthorized access to Ms Chong's email account.
- District Judge sentenced him to 5 months imprisonment.
- Lim appealed and Chief Justice enhanced to 12 months imprisonment (considering the fact that he has used information obtained from Ms Chong's email to stalk and harass her. Lim was completely malicious and vindictive.)

PP v Koh Chee Tong (2016)

- Koh was a compliance officer with United Overseas Bank ("**UOB**") at the time of the commission of the offences.
- Koh owed loan-shark monies. In exchange for reduction in interest charges and extra time to make repayments, Koh agreed to pass names of bank account holders to loan-shark.
- He was charged with 24 counts of unauthorised access to data in the computer system of UOB under section 3(1) of the CMA.
- The prosecution proceeded with four counts, to which he pleaded guilty. The remaining 20 charges were taken into consideration for the purpose of sentence on the application by the prosecution and with the consent of the accused.
- Koh had committed the offences for (a) financial gain and (b) harm was caused to his employer, UOB, because the personal particulars of bank customers were disclosed to unlicensed moneylenders

NB – Offender may also face civil liabilities (eg; sacking by employer without compensation)

http://www.straitstimes.com/singapore/courts-crime/ex-bank-officer-jailed-for-misuse-of-database

Recent Court Case (Sept 2020)

News, wherever you are.
Stay updated with our Telegram service.
JOIN our channel at t.me/todayonlinesg.

We set you thinking
TODAY
WEDNESDAY 30 SEPTEMBER 2020

Cut through the clutter.
Subscribe to our email newsletter for the day's essential news, straight to your inbox.

Singapore World Big Read Opinion Gen Y Speaks Features Visuals Brand Spotlight 8 DAYS

Former DBS employee jailed for selling personal information of 37 customers to data broker

By LOUISA TANG

https://www.todayonline.com/singapore/former-dbs-employee-jailed-selling-personal-information-37-customers-loansharks

Section 4 – Access with Intent to Commit or Facilitate Commission of Offence

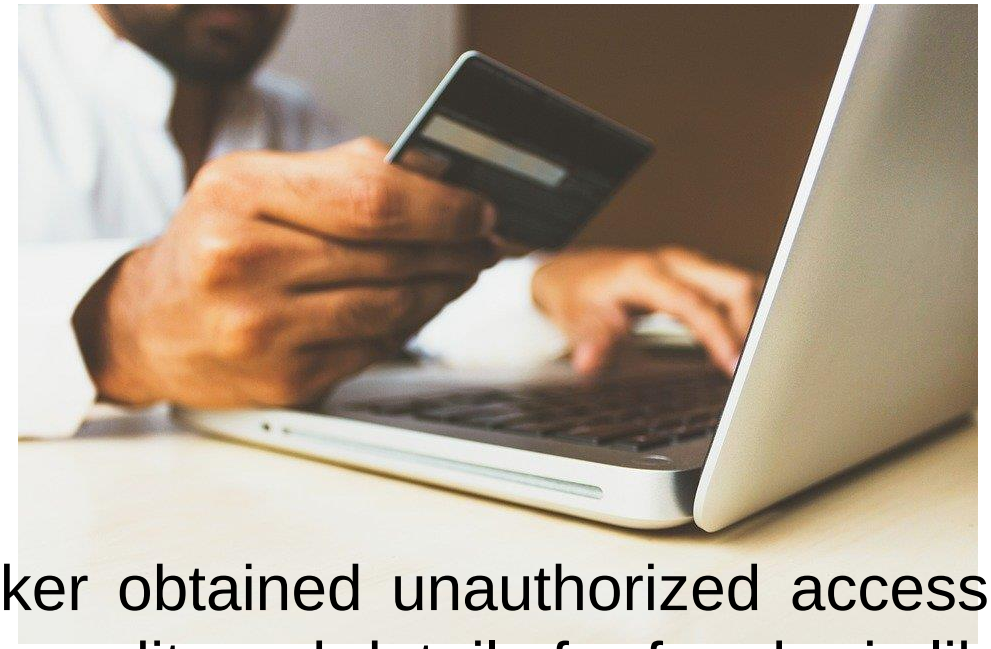
Access with intent to commit or facilitate commission of offence

- **4.** —(1) Any person who **causes a computer to perform any function** for the purpose of **securing access to any program or data** held in any computer **with intent to commit an offence** to which this section applies shall be guilty of an offence.
- (2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years.

- Punishment: fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.
- The dominant consideration which would influence the sentence would be the nature and magnitude of the crime intended and the resultant damage and loss. Unless the value of the property was low or the hurt minor, the offence would generally warrant a custodial sentence (imprisonment).

Section 4 – Access with Intent to Commit or Facilitate Commission of Offence

- Similar to Section 3 but targeted at persons who use computer to secure access in order to commit a further offence and this offence must be one of those listed under Section 4(2).



- For instance if hacker obtained unauthorized access to websites containing credit card details for fun, he is likely to be caught under Section 3. If the hacker had gone shopping with those credit cards thereafter, he would be caught under Section 4 as well.

Ooi May Ling Irene Maria v PP (1998)

- Maria was a bank clerk.
- Maria authorised an internal cash transfer of about S$36,000 (US$22,502.30) from the bank account to her personal saving account with the bank.
- Maria has therefore unlawfully accessed the computer system AND to illegally transfer the monies.
- Judgment by District Court:-

  12 months imprisonment

Ho Poh Leong Nelson v PP (2002)

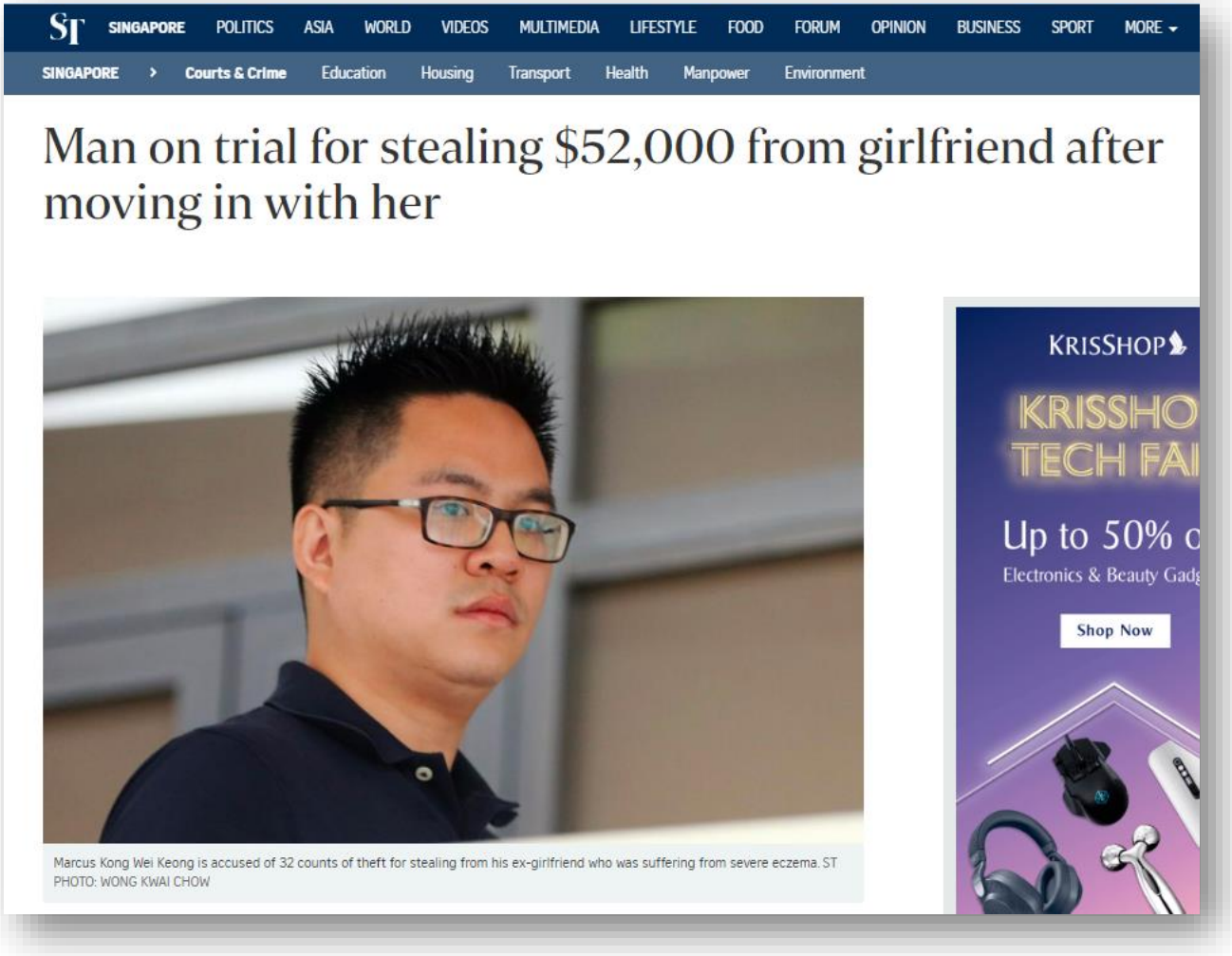
- Nelson gained unauthorised access to the computer server of DBS Internet Banking Service.
- Nelson unlawfully transferred $2,200.
- Court found him guilty under S4(1) of the Computer Misuse Act.

PP v Ricky Widjaja (2015)

- Widjaja was a sports betting trader with Singapore Pools. One of the accused's roles as a sports betting trader was to balance the supply and demand for opposite sides of a bet through adjustment of the odds.
- The accused and his accomplice hatched a plan to misuse their access to Singapore Pools' computer systems to adjust the odds in their favour for brief moments in order to place risk-free bets.
- As a result of their offences, they made a net profit of S$198,500. The accused pleaded guilty to 13 charges under section 4(3) read with section 10(1) of the Computer Misuse Act.
- The accused had conspired with another to commit the offences for (a) financial gain and (b) harm was caused to his employer, Singapore Pools, as it caused a "*loss in confidence in the integrity of Singapore Pools' computer system*"
- Sentenced to 4 years

https://www.straitstimes.com/singapore/courts-crime/ex-sports-betting-trader-who-tweaked-football-odds-jailed

Recent Court Case (2019)



https://www.straitstimes.com/singapore/courts-crime/man-on-trial-for-stealing-52000-from-girlfriend-after-moving-in-with-her

Section 5 - Unauthorised Modification of Computer Material

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.
- (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.

- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
- If damage is caused: fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.
- In assessing sentence, the main considerations would be the intent behind the modification, the extent of damages (if any), the kind of program or data modified, the potential mischief occasioned by the modification, and the difficulty in reinstating the program or data.

Section 5 - Unauthorised Modification of Computer Material

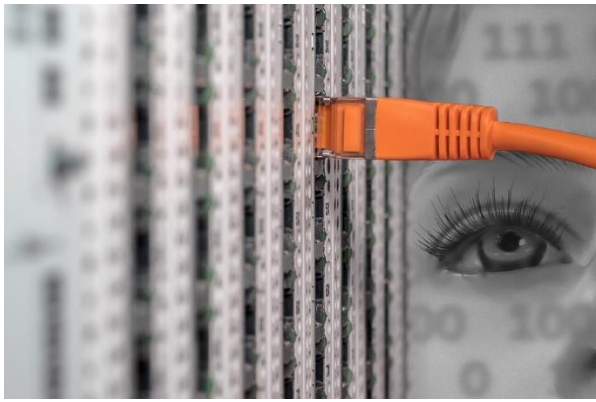
- The modification need not be permanent, even temporary modification if unauthorised, will subject perpetrator to liability under this section.
- Immaterial that the act in question is not directed at any particular program or data or a program or data held in any particular computer. E.g. a person who causes a computer virus to enter into circulation may be prosecuted under this section even though he may not have targeted any specific computer.
- The Court will pay particular attention to the motive and the consequences of the modification.
- Example of when a person may be charged under section 5: where a person uses a debit card he found to make a purchase on eBay. He knew that by doing so, he would cause unauthorised modification to the contents of a computer namely the data stored in the bank's servers such that the online purchase would be approved.

Lim ZhaoMing Edwin v PP (1999)

- Edwin was 18 years old at time of offence
- S3(1) - Edwin secured access to data contained in the Mediacity website web server without the knowledge or authority of Multimedia Division of TCS (Television Corporation of Singapore)
- S5(1) - With the unauthorized access, Edwin modified the homepage, www.mediacity.com.sg to www.mediashity.com.sg
- He also created a new account in such a way that no password was required whenever he logged into the said server using the account and deleted a file to prevent tracing of his wrongdoings.
- As a result of his acts, the Mediacity website was taken off-line for about 10 hours. 80 man hours were spent on system recovery amounting to $12,000 and loss of advertising revenues which was quite substantial.
- Judgment:-

  District Court: 5 months imprisonment

  High Court: enhanced to 10 months imprisonment.



Muhammad Nuzaihan v PP (1999)

- Nuzaihan was just a 17 year old student when he committed these offences.
- S3(1) - Nuzaihan gained access into the computer files in Swiftech's network.
- S5(1) – he executed a program to allow him to gain access to the Internet Relay Chat and successfully created a user account for himself in the server of Swiftech to connect to the IRC. While on the IRC, Nuza indicated to other users on the channel that he was able to compromise a server which ran on a Linux operating system.
- S6(1)(a) – he had earlier applied to Singapore Cable Vision for an internet account but was rejected as the cable modem service was not available to his estate. As such, he decided to gain unauthorised access to the server and configured a backdoor to the server which allowed him to access the server in the future without having to hack into the system again.
- Judgment:-

  District Judge: 2 years and 6 months' probation

  High Court: 6 months imprisonment (Chief Justice)

Recent Court Case

PP v James Raj s/o Arokiasamy (2015)

- The accused carried out computer attacks on several websites under the moniker of *"The Messiah".*
- S3(1) - He hacked into Standard Chartered Bank's server, the fan website of Sun Ho, the pastor of City Harvest Church, three websites linked to City Harvest Church, a Straits Times journalists blog, the PAP Community Foundation website and Ang Mo Kio Town Council's website.
- The accused also scanned and penetration tested various government servers. He pleaded guilty to 39 offences under the CMA and one charge under the Misuse of Drugs Act (Cap 185, 2008 Rev Ed) ("MDA") with a further 119 charges under the CMA and 2 charges under the MDA being taken into consideration for the purposes of sentencing.
- The accused was sentenced to a total of 4 years 8 months. There is no doubt that the accused in that case acted maliciously and harm had been caused to his victims.

http://www.todayonline.com/singapore/messiah-hacker-jailed-56-months

Section 6 – Unauthorised Use or Interception of Computer Service

3 parts:

S6(1)(a)

Secures access without authority for obtaining any computer service

S6(1)(b)

Intercepts without authority any function of a computer

S6(1)(c)

Using the computer to commit an offence under (a) or (b)

Section 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 electro-magnetic, 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*),

- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
- If damage is caused: fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.
- For unauthorised use of computer services, the main considerations in assessing sentence would be the nature and extent of the abuse and damage (if any). For the interception of computer services, the nature of the data intercepted and its use would determine whether a fine or imprisonment is appropriate.

Section 6 – Unauthorised Use or Interception of Computer Service

- "Computer service" is defined in section 2 as including "computer time, data processing and the storage or retrieval of data".
- It is immaterial that the unauthorised access or interception is not directed at any particular program or data or a program or data held in any particular computer. As long as anyone, without authority, knowingly uses or intercepts the computer service, there is liability under this section.
- For example, a perpetrator secures access to a computer within a network server and confidential information is retrieved or used without the knowledge or approval of the owner this would probably be caught under this section.
- Similarly when a perpetrator manages to secure internet access by way of an unauthorised use of a password (say he peeped at someone entering his password) or when he without authority manages to intercept computer or phone services (say broadband services which can be expensive) subscribed by someone else and meant for his sole exclusive use, these acts could constitute offences under this section.

Ong Poh Teng v PP (2001)

- Ong and his co-conspirators committed the offences to obtain pager messages on horse betting tips and information by intercepting radio signals sent from a paging network computer to his program clone pagers.
- Court found him guilty under s 6(1)(b) and (c) of the CMA. 18 months imprisonment.

NB: see also PP v Muhammad Nuzaihan (discussed above)

Section 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,

- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
- If damage is caused: fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.
- The sentence to be imposed would essentially depend on the motive and extent of the obstruction, its consequence and the nature of the computer system.

Section 7 – Unauthorised Obstruction of Use of Computer

- This section was originally intended to deal with E-mail bombing, where the victim receives an enormous amount of electronic mail manifesting in download problems resulting in the system eventually "crashing" causing financial loss and inconvenience.

- The phenomenon of "Spamming" may also be caught under section 7, although this has now to be considered in the light of the recently enacted Spam Control Act (Cap 311A).

- Also referred to as "denial of service" attacks.

Tan Cheng Kang v PP (2000)

HOUSING & DEVELOPMENT BOARD

- The offender was found guilty of three charges under s 7(1)(a) of knowingly interfering without lawful authority or excuse with the lawful use of HDB's Corporate Development Department Compaq 4500R mail server by repeatedly sending 2500 emails to the public mailbox of the computer; to the Quality Service Management mailbox of the computer and to the HDB resale mailbox, resulting in a slowdown.

- The email subject was "letter of complaint – purchase of resale flat" and the contents consisted of about 2 pages of text.
- In the email, the offender complained about the delay of his HDB resale transaction. The offender was frustrated by the delay. He had a clean record.

- District Court – fined $10,000 for each of 3 charges, total $30,000 fine

Section 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.

- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
- Sentencing considerations : sensitivity of computer system and overriding intent behind disclosure of the access code.

*** Section 8 is targeted at unauthorised password disclosure and "password trading" i.e. sell passwords to unauthorized users to enable them access and procure unauthorized usage.**

Section 8A – Supplying, etc., personal information obtained in contravention of certain provisions

Supplying of personal information obtained in contravention of certain provisions

- **8A**.—(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 —
  - (a) 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.

Section 8A – Supplying, etc., personal information obtained in contravention of certain provisions

Supplying of personal information obtained in contravention of certain provisions

- **8A** of CMCA criminalises acts that deal with personal information which the wrongdoer knows or has reason to believe that the information was obtained by committing a computer crime (s3, s4, s5 & s6). The act of obtaining or dealing with such personal information will be an offence, as well as supplying, offering to supply, transmitting or making available the personal information to facilitate the commission of any crimes.
- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.

- **Section 8A is targeted at <u>dealing in hacked personal information</u> to commit any offence**
- ***** Example: criminals trade in hacked credit card information, even though they are not responsible for hacking the personal information.
- NB: theft of personal data may constitute offence under Personal Data Protection Act.

Section 8B – Obtaining, etc., items for use in certain offences

Obtaining items for use

- **8B**.—(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.
- First offence punishment: fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both
- Subsequent offence punishment: fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
- **Section 8B is targeted at supplying, dealing in "hacking tools" etc to commit computer crimes.**
- * Example of hacking tools: malware and port scanners.

Section 9 - Enhanced punishment for offences involving protected computers

9. —(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 —

- (*a*) 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**.

Enhanced punishment

9. —(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
- imprisonment for a term not exceeding 20 years
- or to both.

Section 9 only applies to the commission of an offence under section 3, 5, 6 or 7

NB also that the Court can order a person convicted of a CMA offence to pay compensation to any person for any damage caused to the computer, program or data.

Section 10 - Abetments and attempts punishable as offences

Abetments and attempts punishable as offences

- **10.** —(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.

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

Territorial Nature of CMA

Territorial scope of offences under this Act

- **11**.—(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.

Territorial Nature of CMA

Territorial scope of offences under this Act

- **11**.—(4) 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 [such as communications and transport infrastructure or public utilities];
  - (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.

Mitigating Factors
(To say “I am sorry…”)

Any information or evidence presented to the court regarding the defendant or the **circumstances** of the crime that might result in reduced charges or a lesser sentence.

Good Mitigating Factors

- “First Offence” Submission
- Community Service / Good Public Service / Good student
- Plea of Guilt at earliest opportunity
- Shown remorse by doing certain acts (eg; returned stolen money)
- Cooperation with enforcement authorities

Poor Mitigating Factors

- Ignorance of the law
- “Sole Bread winner” theory
- Intoxication

Photo by: https://tinyurl.com/y5txw3r8

(Self- Reading) Perpetrators of computer crime

- The perpetrators of computer crime are the same as they are for any other type of crime – thrill seekers wanting to take on a challenge, common criminals seeking financial gain, industrial spies trying to gain a competitive advantage and terrorists seeking to cause destruction in order to bring attention to their cause.
- Each type of perpetrator has different objectives and access to varying resources and each is willing to accept different levels of risks to accomplish the objective.
- Knowing these parameters for each set of likely attackers is the first step toward establishing effective countermeasures.
- These are shown in more detail in the next two slides

Classification of perpetrators of computer crimes

Type of Perpetrator	Objective	Resources	Level of Risk acceptable to perpetrator	Frequency of attack
Hacker	Tests limits of system and gain publicity	Limited	Minimal	High
Cracker	Cause problems, steal data and corrupt systems	Limited	Moderate	Medium
Insider	Financial gain and disrupt company's information systems	Knowledge of systems and passwords	Moderate	Low

Classification of perpetrators of computer crimes

Type of Perpetrator	Objective	Resources	Level of Risk acceptable to perpetrator	Frequency of attack
Industrial spy	Capture trade secrets and gain competitive advantage	Well-funded and well-trained	Minimal	Low
Cyber criminal	Financial gain	Well-funded and well-trained	Moderate	Low
Cyber terrorist	Cause destruction	Not necessarily well-funded or well-trained	Very high	Low

End Of Lecture