Computer Law and Investigation ST2502

Assignment: (1/2)

Class: DISM/FT/1B/07

Student Number	Full Name
2123602	Shushant Shashwat
2123222	Urias Francis Paul John Bato
2107095	Md Amirul Adeeb
2123516	Chua Mun Ling
2123392	Marcus Wong Yu Xuan

Submitted to: Ms Adeline Lee

Date of submission: **Thursday 10 February 2022, 5.30 pm**

Executive Summary

In the featured article, the wrongdoer(s) committed many offences under the Singapore Computer Misuse Act (CMA). Each of these offences has its section, with each section having its own set of consequences and punishments. Furthermore, the punishments for the wrongdoer(s) can be enhanced by other sections, such as section 11 of the CMA.

Singapore's CMA can be used to prosecute wrongdoers that commit crimes that vary in terms of the crime committed. The punishments differ based on the offences committed under the different sections of the CMA. The sections consist of sections 3,5,6 and 7 and get increasingly detrimental in terms of the prosecutions and damage costs.

Preventive and practical measures should be implemented to prevent computer crimes. Such measures include restricting access to computer systems and using Intrusion Detection Systems (IDS). Measures are also taken under the Cybersecurity Code of Practice to ensure the protection of Singapore's Critical Information Infrastructure (CII). These measures would ensure confidential data and information stored on computer systems are kept secure and away from cybersecurity threats.

MyRepublic has to comply with the Data Protection Provisions in parts 3 to 6A of the PDPA and the common law of confidentiality. Since the confidentiality breach, a fine penalty will be imposed on them.

Table of Contents

1. Introduction

The personal data of nearly 79,400 MyRepublic mobile phone users may have been hacked. On August 29, MyRepublic discovered unauthorized access to data on a third-party storage platform used to store the personal data of mobile customers. According to the mobile operator, access to data storage is already guaranteed. The access took place on a platform used to store mobile customers' personal data and mitigate risk, the ISP activated its cyber incident response team, which included a team of external KPMG consultants to "work closely" with internal IT and cyber teams to resolve the issue.

2. Offences committed under the Computer Misuse Act (CMA)

The first of the possible offences of the featured article is a section 3 offence. Section 3 of the CMA states that “any person who knowingly causes a computer to perform any function to secure access without authority to any program or data held in any computer shall be guilty of a section 3 offence”. In the featured article, the wrongdoer(s) got unauthorised data access to a third-party data storage platform that was used to store the personal data of mobile customers. Based on the above, the wrongdoers are guilty of a section 3 offence, because they secured access to data on a computer, without being authorised to do so. A section 3 offence causes the offender to be liable to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years, or both. In case of a second or subsequent conviction, the offender is liable to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years, or both. Furthermore, 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 both.

The second of the possible offences of the featured is a section 4 offence. Section 4 of the CMA states that “any person who causes a computer to perform any function to secure 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”. The section applies the offences involving property, fraud, dishonesty, or which causes bodily harm, and which is punishable on conviction with imprisonment for a term not less than 2 years. In the featured article, the wrongdoer(s) could use the stolen information for many other offences. One offence the wrongdoer(s) could use is identity fraud, as the personal data of customers could allow the wrongdoer(s) to create new accounts in the victim’s name to conduct fraudulent activities. Moreover, even if the wrongdoer(s) are unable to benefit from your data, they can just sell it to someone else that can. Based on the above, the wrongdoers are guilty of a section 4 offence, because they could have used the stolen personal data for other offences. A section 4 offence causes the offender to be liable for a fine not exceeding $50,000, imprisonment not exceeding 10 years or both. Furthermore, this section will still apply to offenders even if the access is authorised, and whether the offence is committed at the same time when access is secured or any other time.

Another offence to take note of in the featured article is section 11. Section 11 of the CMA states that “where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, a person convicted of the 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”. A computer is 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; the existence or identity of a confidential source of information relating to the enforcement of a criminal law; the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services. In the featured article, the victim of the offence was MyRepublic, which the wrongdoer(s) ought to have known is a company that provides services directly related to communications infrastructure, because MyRepublic is a mobile operator and Internet service provider. Based on the above, the wrongdoers are guilty of a section 11 offence, but they committed an offence involving protected computers. This means that instead of punishments explained in sections 3, 5, 6 and 7, the punishments will be enhanced because the offence is more serious.

3. How CMA is used to prosecute wrongdoers that commit computer crimes

Singapore's Computer Misuse Act can be used to prosecute wrongdoers that commit computer crimes that vary in terms of punishments and prosecutions which depends on the section of the CMA the wrongdoer has violated.

Unauthorised access to computer material

The first would be the unauthorised access to computer material which is section 3 of the CMA. Section 3 also deals with users who exceed authority and access parts of a system officially denied to them. One court case example would be Public Prosecutor (PP) v Koh Chee Tong in 2016. Koh was a compliance officer with United Overseas Bank (UOB) at the time of the commission of the offence. Koh owed loan-shark monies. In trade for lessening in interest charges and additional time to form reimbursements, Koh concurred 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 sentence on the application by the prosecution and with the consent of the accused. Koh had committed the offences for financial gain and harm was caused to his employer, UOB because the personal particulars of bank customers were disclosed to unlicensed moneylenders.

Access with intent to commit an offence

The second would be accessing with intent to commit or facilitate the commission of an offence which is section 4. It is similar to section 3 but is aimed at people who use computers to get access to secure information to commit a subsequent crime, which must be one of those mentioned in section 4(2). One case court example would be PP v Ricky Widjaja in 2015. Widjaja worked for Singapore Pools as a sports betting trader. One of the accused's responsibilities as a sports betting trader was to modify the odds to balance supply and demand for opposite sides of a bet. The accused and his accomplice devised a scheme to exploit their access to Singapore Pools' computer systems to manipulate the odds in their favour for a brief period to place risk-free bets. Due to 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 CMA. The accused had conspired with another to commit the offences for financial gain and harm was caused to his employer, Singapore Pools, as it caused a "loss in confidence in the integrity of Singapore Pools' computer system".

Unauthorised modification of computer material

The third would be the unauthorised modification of computer material which is section 5. This section does not require permanent modifications. A case court example would be Muhammad Nuzaihan v PP in 1999. He gained access to the computer files in Swiftech's network which is also under section 3(1). Under section 5(1), Nuzaihan executed a program to allow him to gain access to the Internet Relay Chat (IRC) and succeeded in establishing a user account on the Swiftech server so that he could connect to the IRC. He had previously applied for an internet account with Singapore Cable Vision but had been turned down since the cable modem service was not available in his estate. As a result, he planned to acquire unauthorised access to the server and set up a backdoor that would allow him to access the server without having to hack into the system again in the future which is also under section 6(1)(a) which is the unauthorised use of computer services. The district judge sentenced him to 2 years and 6 months' probation and the high court sentenced him to 6 months imprisonment.

Unauthorised obstruction of use of computers

The fourth would be the unauthorised obstruction of use of computers which addresses E-mail bombing or spam. A case court example would be Tan Cheng Kang v PP in 2000. The topic of the email was "letter of complaint – purchase of resale flat," and it had around two pages of text. In the email, the offender complained about the delay of his HDB resale transaction and was frustrated by the delay. The offender was found guilty of three counts of knowingly interfering with the lawful use of HDB's

Corporate Development Department Compaq 4500R mail server without lawful authority or excuse by repeatedly sending 2500 emails to the computer's public mailbox, the computer's Quality Service Management mailbox, and the HDB resale mailbox, causing a slowdown. In the district court, he was fined $10,000 for each of 3 charges which totalled up to $30,000.

4. Measures to prevent computer crimes, misuse of computer data and computer network

With occurrences of computer crimes, laws are passed to punish the wrongdoers. To better protect computer systems from computer crime, misuse of computer data and computer networks, preventive and practical measures can be implemented in the first place. Under the Cybersecurity Code of Practice for Critical Information Infrastructure (CII) under the Cybersecurity Act 2018 (Act 9 of 2018), measures are taken to protect Singapore's CIIs. Other possible measures include restricting access to computer systems and to use Intrusion Detection systems (IDS) devices or software.

Regarding the Cybersecurity Code of Practice Section 5, Protection Requirements, it indicates measures that must be taken by Critical Information Infrastructure Owners (CIIO) under the act. For access control, CIIO must ensure any access to the CII is restricted to authorised personnel and activities. For system hardening, CIIO must establish security configurations for operating systems, applications, and network devices. The CIIO must review each security configuration once every 12 months from the time of designation of the CII and ensure effectiveness against cybersecurity threats. For remote connection, the CIIO must ensure all remote connections to the CII have effective cybersecurity measures in place to prevent and detect unauthorised access. For removable storage media, CIIO must exercise strict control including disabling external connection ports supporting removable storage media, enabling only when required. Lastly, for vulnerability assessment and penetration testing, CIIO should conduct vulnerability assessments for the CII to identify security and control weaknesses. The assessment should be done within 12 months from the date of notice and at least once every 12 or 24 months from the time of the previous assessment. The date of notice is defined to be the date that the owner of a computer or computer system receives a written notice by the Commissioner to designate the computer or computer system as a Critical Information Infrastructure. Penetration testing should also be done for CII systems to validate the cybersecurity posture of the CII.

Other than the measures taken and stated above, other measures should be taken to protect computer systems from computer crimes. One measure is to restrict access to computers which includes only allowing authorised users to have access to the computer system and data stored in the computer. Access to the terminals on the network should also be restricted. One way to restrict access is to ensure that access is only possible with a strong password known only to authorised users. Additional security can also be added to confidential files on the computer system by adding passwords to the files. This ensures that confidential information and data are kept secure. Also, ensure that computers are not left connected to the internet when not in use as this may allow access via an internet connection which may compromise the whole system. Access privileges can also be set to allow trusted company staff or only the owner of the computer to have access to confidential information and make changes. This will ensure that important information stored in a computer system used and shared by many users will be kept safe. With access privileges set, in case of any data leak or misuse of data, investigations can start from this small group of privileged users before considering the possibilities of acts being done by unauthorised users.

Another measure that can keep computer systems and their data safe is to use Intrusion Detection Systems (IDS) devices or software. IDS helps to indicate when an internal attack is taking place or when a hacker obtained access to the system. IDS can identify statistical deviations, point out unusual behaviour within the network and can also be programmed to detect when certain areas of the network are tempered with. There are different types of IDS. The Host-Based IDS (HIDS) is deployed on a particular remote computing device and designed to protect it against internal and external threats. HIDS have the ability to monitor network traffic to and from the machine, observe running processes, and inspect the system's log. Another type of IDS is the Network-Based IDS (NIDS) which is designed

to monitor an entire protected network. It has visibility into traffic in the network and makes decisions based on packet metadata and contents. Its wider viewpoint gives more context and the ability to detect widespread threats. IDS helps to analyse the quantity and types of attacks that information can be used to change the security system and implement more effective security controls.

With the above measures put in place, it will ensure some security to prevent attackers from obtaining confidential data. Many other measures such as firewall and user training which can also help to keep computer systems safe are not mentioned. Implementing these measures will lead to lesser successful computer crimes.

5. Whether PDPA and the common law of confidentiality can resolve issues of privacy

5.1 Personal Data Protection Act

Data privacy is about the voluntary sharing of information. Keeping data private means keeping it isolated within the person-service relationship, and not having it be used in ways that are not consented to and known by individuals. Individuals have to know how their personal data is being used, stored and shared to determine that their personal data are being kept private. The Personal Data Protection Act (PDPA) is put in place to control the collection, use and disclosure by organisations in a way that recognises both the right of individuals protects their personal data and the need for organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

MyRepublic is required to comply with the Data Protection Provisions in Parts 3 to 6A of the PDPA. Regarding the compliance of the data protection provisions. They are to be responsible for the personal data they acquire. There are some main obligations that MyRepublic has to observe regarding the collecting, using or sharing of personal data.

According to PDPA sections 13 to 17, An MyRepublic has to ask permission from the individual before collecting, using or sharing personal data for a purpose. Section 18 states that they can only collect, use or reveal the information only if the situation is considered suitable and sensible and if applicable.

Section 20 states that the organization has to inform the individual of the reasons for collecting, using or disclosing before doing so. MyRepublic has a website that includes its privacy policy. According to Sections 21,22 and 22A, upon request of the customers, MyRepublic has to provide individual customers with their personal data and the manner it has been used or disclosed and corrects a mistake or an exclusion in an individual's personal data in possession of MyRepublic.

MyRepublic also has to cease to retain documents containing any personal data related to the individual customers as soon as the purpose for which the personal data was collected is no longer needed or necessary for MyRepublic to carry out their business and serve the customers according to section 25.

PDPA section 24 tells us that MyRepublic has to protect personal data in its possession or under its control by making reasonable security measures to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and the loss of any storage medium or device on which personal data is stored. However, they failed to do so and faced a data breach.

When faced with a data breach, MyRepublic must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable according to section 26A to 26E. The recent MyRepublic data storage breach where nearly 80 000 customers personal information is accessed is a notifiable data breach as it is of a significant scale and the customers' identities could be hijacked.

.
MyRepublic could be fined up to 10 per cent of their annual turnover in Singapore, or $1 million. Individuals who suffer loss or damage directly as a result of a contravention of Parts 4, 5, 6 or 6A of the PDPA by an organisation may commence civil proceedings against the organisation.

5.2 Common Law of Confidentiality

The general position is that if the information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent. The information must also be confidential and not made available to the public. There also must be unauthorised use of the information.

MyRepublic list of customers identity verification documents including scanned copies of NRICs of customers and other personal data such as mobile numbers are not in the public domain and are confidential. That information belongs to individual customers. There is an obligation of confidence because the information was given for a limited purpose which is to offer and deliver products and services to the customers. From the article, there is no evidence that any personal data has been misused for now. MyRepublic also says that it will provide affected customers a complimentary credit monitoring service through Credit Bureau Singapore to safeguard against identity theft. If there is any personal data being misused, customers affected can apply to court for an injunction and either damage or account of profits if they can demonstrate the harm they receive such as identity theft or fraudulent credit card use.

Conclusion

In conclusion, multiple statutes are used when dealing with computer crime, such as the Computer Misuse Act. In the featured article, there were many offences under the different statutes. There are different punishments for each of these offences, with differing levels of severity. Due to the increase in computer usage, practical measures should be taken to prevent computer crime, and the misuse of computer data and computer networks. Some practical measures include the Cybersecurity Act, restricting access and use of Intrusion Detection Systems. In the featured article, the company attacked, MyRepublic, which needed to adhere to the Cybersecurity Act as a practical measure against any computer crime and unauthorised access. Lastly, the Personal Data Protection Act and the law of Confidentiality resolves issues related to personal privacy and information. In the featured article, the data that was compromised was considered personal data, which means that the Personal Data Protection Act should be followed.

References

Anon, PDPC: PDPA Overview. *Personal Data Protection Commission*. Available at: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act [Accessed February 9, 2022].

Anon, Search within legislation. *Singapore Statutes Online*. Available at: https://sso.agc.gov.sg/Act/CMA1993 [Accessed February 9, 2022].

B. Lutkevich, 2021. What is an intrusion detection system (IDS)? Definition from SearchSecurity. SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system [Accessed February 9, 2022].

Check Point Software, 2021. What is an Intrusion Detection System (IDS)? Available at: https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/# [Accessed February 9, 2022].

Chee, K. & Chia, O., 2021. Hackers possibly stole personal data of 79,400 MyRepublic customers, including copies of nrics. *The Straits Times*. Available at: https://www.straitstimes.com/tech/tech-news/hackers-stole-personal-data-of-79400-myrepublic-customers-including-copies-of-nrics [Accessed February 9, 2022].

Computer Hope, 2020. How to prevent unauthorized computer access. Available at: https://www.computerhope.com/issues/ch000464.htm [Accessed February 9, 2022].

Craig W., 2008. Access Restriction | An Introduction to Systems Auditing. *ScienceDirect.* Available at: https://www.sciencedirect.com/topics/computer-science/access-restriction [Accessed February 9, 2022].

CSA Singapore, 2018. CYBERSECURITY ACT 2018 (ACT 9 OF 2018) CYBERSECURITY CODE OF PRACTICE FOR CRITICAL INFORMATION INFRASTRUCTURE (FIRST EDITION – SEPTEMBER 2018). Available at: https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_COP/cybersecurity-code-of-practice-cii-dec-2019.pdf [Accessed February 9, 2022].

Lee M., (n.d.). Ways to Prevent Computer Crime. *Techwalla.* Available at: https://www.techwalla.com/articles/ways-to-prevent-computer-crime [Accessed February 9, 2022].

Palo Alto Networks, (n.d.). What is an Endpoint? Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint [Accessed February 9, 2022].

Singapore Statutes Online, 2018. Cybersecurity Act 2018. Available at: https://sso.agc.gov.sg/Acts-Supp/9-2018/?ProvIds=P13-#pr7- [Accessed February 9, 2022].

Singapore Statutes Online (2012). *Personal Data Protection Act 2012 - Singapore Statutes Online*. [online] Agc.gov.sg. Available at: https://sso.agc.gov.sg/Act/PDPA2012.

ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT. (2013). [online] Available at: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en.