Computer Law and Investigation ST2502

Assignment: (1/2)

Class: DISM 1B07

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

Submitted to: Ms Adeline Lee

Date of submission: **Thursday 2 Dec 2021, 5.30pm**

Table of Contents

Page

Executive Summary

Computer Crime is the use of a computer as an instrument to further illegal ends. There are various types of cybercrime in Singapore, and six of the computer crime offences are highlighted in the Computer Misuse Act (CMA). The complementary of the CMA is the Cybersecurity Act (CA).

Singapore continues to see an increase in cybercrime attacks as it becomes almost half of crime committed. These computer crimes are committed by different groups of criminals such as script kiddies, hacktivists, insiders, “black hat” hackers or crackers, cyberterrorists, and cybercriminals. These groups have different motivations which is based on their attributes, funding and resources, intent, and motivations.

Repercussions of cybercrime can have varying effects on individuals and corporates if left undetected. On personal level, cybercrime can cause violation of personal data and privacy. On corporate level, operations may be disrupted, companies may suffer great losses and reputational damage. Precautions should be taken by both individuals and companies to lower chances of successful cybercrime attacks.

With the increase in the worldwide internet usage and the high incidence of Internet-related crimes, the Singapore government has identified cybercrime as a serious social and economic problem that the country must tackle. However, to provide a comprehensive overview of the Internet-related crime in Singapore, a holistic approach is required that involves the various dimensions of this problem. Therefore, this study aims to investigate the state of cybercrime in Singapore and to identify the causes of these crimes as well as to identify the potential solutions for these cybercrimes. The research findings revealed certain issues in the cybercrime in Singapore, such as the high rate of cybercriminals involved in cybercrimes, the increased use of the Internet for business development, online scams & cyberthreats.

Introduction

The purpose of this report is to provide the public with an overview the current state of the issue of cybercrime Singapore, as well as to provide the information needed to help the public make informed decisions regarding their personal information security.

The term cybercrime is ambiguous. The dictionary defines cybercrime as any crime that involves digital information. Cybercriminals are any criminals that attack or use cybertechnology. However, cybercrime has historically been very difficult to fully define due to the broad and ever-changing nature of the Internet and digital systems.

Computer Crime and the various types of Computer Crime

Cybercrime, also called computer crime, is the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. The main types of computer crimes are found in the Computer Misuse Act (CMA).

The first offence in the CMA is Section 3, which is unauthorised access to computer material. This means that an offence is committed by anyone who causes a computer to perform any function for the purpose of gaining unauthorised access to a program or data stored on a computer.

The second offence in the CMA is Section 4, which is access with intent to commit or facilitate commission of offence, regardless of authorisation. This means that an offence is committed by anyone who has access to any program or data and uses the access to commit another offence. This applies to offences involving property, fraud, dishonesty or which causes bodily harm.

The third offence in the CMA is Section 5, which is unauthorised modification of computer material. This means that an offence is committed by anyone who intentionally causes an unauthorised modification of the contents of any computer.

The fourth offence in the CMA is Section 6, which is the unauthorised use or interception of a computer service. This means that an offence is committed by anyone that pirates any computer service; intercepts or causes to intercept without authority, any function of a computer using electro-magnetic, acoustic, mechanical, or any other device; or use a computer or any other device to pirate or intercept.

The fifth offence in the CMA is Section 7, which is the unauthorised obstruction of use of computers. This means that an offence is committed by anyone that obstructs the lawful use of a computer; or prevents access to or impairs the effective use of any program or data stored in a computer, such as email bombing.

The sixth offence in the CMA is Section 8, which is the unauthorised disclosure of access code. This means an offence is committed by anyone that reveals any means of gaining access to programs or data shall be guilty of an offence if they did it for wrongful gain, any unlawful purpose, or knowing that it will cause wrongful loss to any person. Section 8A applies to personal data while Section 8B applies to hacking tools used.

Another important act is the Cybersecurity Act. It seeks to establish a framework for the protection of critical information infrastructure against cybersecurity threats, the taking of measures to prevent, manage and respond to cybersecurity threats and incidents in Singapore, and the regulation of providers of licensable cybersecurity services.

Prevalence of Computer Crime in Singapore

Cybercrime continues to be on the rise in Singapore, with 5,430 cases reported in 2017, according to the Singapore Police Force. Between 2016 and 2017, the percentage of cybercrime cases grew from 15.6% to 16.6% of total crimes, even as overall crime numbers fell. (Gosafeonline, *CSA: Gosafonline: Crimewatch)*

SINGAPORE: Cybercrime accounted for 43 per cent of all crime in Singapore last year, with the COVID-19 pandemic being a key factor in online threats. According to an annual report released by the Cyber Security Agency of Singapore (CSA) on Thursday (Jul 8), there were 16,117 cases of cybercrime last year, up from 9,349 cases recorded in 2019. It mainly affected small- and medium-size enterprises (SMEs) from sectors such as manufacturing, retail, and healthcare. This is primarily due to Covid-19 pushing businesses to be more digital, increasing the chances for data breaches to occur. (Cindy Co @CindyCoCNA)

Profile and intention of wrongdoers

There is wide array of different types of wrongdoers who commit computer crimes for different motivations. As with any other type of crime, computer crime is committed by thrill seekers seeking a challenge, common criminals seeking financial gain, industrial spies seeking a competitive advantage and terrorists seeking to cause destruction in their target areas. These different groups of wrongdoers can vary widely, based on attributes, funding and resources, intent, and motivations.

The first group are known as Script kiddies. Script kiddies are individuals who want to attack computers, yet they lack the knowledge of computers and network needed to do so. They can easily download automated hacking software from websites on the Internet. Script kiddies are motivated by peer competition and often have no regard for the consequences of their hacking.

The second group are referred to as Hacktivists. The term hacktivist refers to a collective of criminals who collaborate in the pursuit of political goals. Hacktivists tend to attack whole industries, but they may also attack specific organizations, especially if their political views conflict with their practices. In many cases, hacktivists support causes ranging from free speech to civil rights, from religious freedom to political opposition.

The third group are Insiders. Insiders could be employees working in the company, contractors, and business partners. have the capabilities, motivations, and privileges needed to steal important data. 34% of the data breaches involve internal actors and 71% of them are motivated by money. (Vernon.com,2019). Most cases of cyber-attacks committed by insiders are due to being disgruntled over an upcoming job termination or through fake transactions for a stock trader.

The fourth would be cyberterrorists. They are individuals who attack a nation’s network and computer infrastructure to cause disruption and panic among citizens. Their targets may include a small group of computer and networks that can affect the largest number of users, such as computers that control the electrical power grid of a state or region and their intent is always malicious.

The fifth group are crackers also called “black hats” hackers. A black hat hacker is a hacker who's breaking into a computer system with malicious intent. They lack ethics, sometimes violate laws, and may compromise an organization's confidentiality, integrity, or availability. They have intentions to cause problems, steal data and corrupt systems for personal gain or merely to take up the challenge and show off. An example of cracking would be jailbreaking whereby hackers removes restrictions in a software or device and perform advanced functions.

The last group are cybercriminals, often working in organised groups, they commit malicious activities on digital systems or networks. They have intentions to steal sensitive company information or personal data and generate profit. Cybercriminals perform attacks on broad masses of victims who visit similar platforms, have similar online behaviour, or used similar programs.

Repercussion of Computer Crimes

Computer crimes invade individuals' privacy and the security of their data, particularly hacking, identity theft, data theft, financial fraud, medical fraud and disclosure of sensitive information such as messages or video and audio recordings. (Norton 2016) Psychological approaches such as impersonation, phishing, spam and hoaxes are used to persuade victim to provide information or take action.

Without your knowledge, spyware runs in the background while it captures and stores keystrokes to search for useful information such as password, credit card information or personal information, which can lead to credit card fraud and online identity theft. As a result, if individuals were to fall into such traps, there will be some immediate effects. Firstly, they will lose money due to online theft. Secondly, they might lose reputation as their personal information are disclosed. Lastly, their files can get corrupted or deleted due to malware.

Hence, there is need for individuals to be vigilant and have sufficient knowledge on cybercrime and take precautions to prevent attacks and keeping the rate of cybercrime low. Precautions that individuals can take will be to keep software and operating system updated, use anti-virus software and strong passwords, check for credibility of emails before entering any URL attached and never enter or send personal information via phone or email unless receiver is known to be credible.

Many computer crimes go undetected and unreported because they are so well-hidden. Cybercrime is a trillion-dollar business. Cybercriminals are spending more on innovation compared to corporation on cybersecurity. (Axim, 2018)

At the corporate level, consequences of hacking include data theft and damaging of data to sabotage the company. Hacker gain access to a computer to steal confidential and valuable information such as credit cards information or future of the company which can be sold to a competitor company. Hackers destroy data or can encrypt the data and held ransom until they are paid. In rare cases, they can even command and control devices to destroy physical equipment. (Melendez,2019) They usually do it for momentary gain or ideological reasons. Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (Varonis,2021)

Firstly, companies' operation will be disrupted. During cyber-attacks, company’s normal activities might be stopped. Threat actors usually do so by infecting computer systems with malware that delete highvalue information. (Logan,2021) A denial of service attack halts a company's Web servers entirely, resulting in clients and customers being denied access to any online service provided by a company.

Productivity of the company will be reduced. Post-attack cleans up diverts resources away from normal activities. For example, time, money, and other resources. Such resources have to be spent on recovering from loss caused by computer crimes instead of spending on the corporate development.

During a cyber breach, companies must incur costs to repair affected systems, networks, devices and the expertise required. Ransomware also can prevent workers from accessing IT systems unless the company pays off a hacker, can also create a major financial burden. The average cost of a cyber security attack for organisations in Singapore stands at approximately S$1.7 million per breach, with businesses on “high” alert in 2020. (Henderson,2020)

It will also cause reputational damage to corporation. Cyber-attacks on a company can damage the business reputation and diminish the trust customers or investors have for it. This could lead to the loss of customers and the ability to gain new customers, loss of sale and reduction in profits.

Precautions that corporates can take is to back-up data, activate data encryption, replace passwords with passphrases, implement security policies and provide cybersecurity training for employees.

Computer Crime Investigations

Police investigations provide unique knowledge about criminal networks and their members due to the wide use of intrusive investigative methods such as wiretaps and IP taps, observations, undercover policing, and house searches.

Wiretapping is the surreptitious electronic monitoring of telephone, telegraph, cellular, fax or Internet-based communications. Wiretapping is achieved either through the placement of a monitoring device informally known as a bug on the wire in question or through built-in mechanisms in other communication technologies. Enforcement officials may tap into either for live monitoring or recording. packet sniffers -- programs used to capture data being transmitted on a network – are a commonly-used modern-day wiretapping tool. A variety of other tools, such as wiretap Trojans, are used for different applications.

Undercover policing means that a police officer pretends to be a regular citizen, while concealing his identity as a police officer. Undercover police officers may assume a false identity for a time to get information out of unsuspecting suspects, such as cyber criminals.

For house searches, police officers do not need a warrant to search a house if the police officer has good grounds for believing that any stolen property will be removed from the premises by the time the search warrant is obtained.

For any crimes under the CMA, any police officer can arrest any person suspected of committing an offence without a warrant.

The Singapore Police Force (SPF) Cybercrime Command established in 2015 integrates cyber-related investigation, forensics, intelligence, and crime prevention capabilities improving coordination and coherence of SPF's response to cybercrime. SPF Cybercrime Command also oversees Cybercrime Response Teams based in every Police Land Division who assist investigation officers in responding to reports of cybercrime. The Cybercrime Response Teams assist by collecting and processing digital evidence and conducting forensic analysis of computers and mobile phones. SPF have new initiatives to improve its cybercrime investigation capabilities. An example is the Digital Evidence Search Tool (DIGEST) which automate the forensic processing of voluminous data. The tool reduces the processing time for digital evidence, helping investigation officers to follow up on lead expeditiously and solve cases in shorter time.

Conclusion

With increased digitalisation and use of technology in Singapore, cybercrime will become increasingly common. Cybercriminals will find new methods to gain access to data and IT systems to reach their goals and to reap the profit out of those stolen data or information. To prevent cybercriminals from achieving their goals and lowering the chances of successful cyber-attacks, precautions should be put in place and having the relevant knowledge is the key to lowering prevalence of cybercrimes happening. Investigations and implementation of measures or laws in response to cybercrimes will deter cybercriminals and prevent more cases of cybercrime from happening, making the cyberspace a safer environment.

Reference List

Anon, CSA: Gosafonline: Crimewatch. *Cyber Security Agency*. Available at: https://www.csa.gov.sg/gosafeonline/Resources/Crimewatch [Accessed November 28, 2021].

Anon, Computer Misuse Act. *Singapore Statutes Online*. Available at: https://sso.agc.gov.sg/Act/CMA1993?ProvIds=P1II-#pr5- [Accessed November 30, 2021].

AXIM (2018) If so much cybercrime is undetected and unreported, what's the answer? [Online]. Available at: https://www.aximglobal.com/blog/if-so-much-cybercrime-is-undetected-and-unreported-whats-the-answer/ (Accessed: 30 Nov 2021)

Cindy Co @CindyCoCNA, Cybercrime made up 43% of overall crime in 2020; more online threats linked to COVID-19. *CNA*. Available at:

Cybercriminals (2019) [online] Trendmicro Available at: https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals [Accessed November 30, 2021]

Cybersecurity Act (2018) [online] Cyber Security Agency Available at: https://www.csa.gov.sg/legislation/cybersecurity-act [Accessed November 30, 2021]

https://www.channelnewsasia.com/singapore/cybercrime-hacking-phishing-online-crimes-covid-19-1984866 [Accessed November 28, 2021].

Dennis, M.A., Cybercrime. *Encyclopædia Britannica*. Available at:https://www.britannica.com/topic/cybercrime [Accessed November 28, 2021].

Henderson,J.(2020) Security attacks cost Singaporean businesses $1.7M per breach [Online]. Availabe at: https://www.channelasia.tech/article/670400/security-attacks-cost-singaporean-businesses-1-7m-per-breach/ (Accessed: 30 Nov 2021)

Jelen S., 2021. SecurityTrails: Hacker vs Cracker: Main Differences Explained [online] SecurityTrails. Available at: https://securitytrails.com/blog/hacker-vs-cracker [Accessed November 29, 2021]

Logan,M.(2021) 6 Ways Cybercrime Impacts Business [Online]. Available at: https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx (Accessed: 30 Nov 2021)

Melendez,S.(2019) The Effects of Computer Hacking on an Organization [Online]. Available at: https://smallbusiness.chron.com/effects-computer-hacking-organization-17975.html (Accessed: 30 Nov 2021)

National Cybercrime Action Plan (2016) [online] Ministry of Home Affairs (MHA) Available at: https://www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf (Accessed: 30 Nov 2021)

Norton (2016) The personal impact of cybercrime [Online] Available at: https://us.norton.com/internetsecurity-emerging-threats-personal-impact-cybercrime.html (Accessed: 1 Dec 2021)

Rosanes M., 2021. Ten ways to protect your business from cyber attacks. [online] Insurance Business Australia Available at: https://www.insurancebusinessmag.com/au/news/breaking-news/ten-ways-to-protect-your-business-from-cyber-attacks-249955.aspx [Accessed November 30, 2021]

Shea S., Lutkevich B., 2021. What is Computer Cracker? [online] Search Security. Available at: https://www.techtarget.com/searchsecurity/definition/cracker [Accessed November 29, 2021].

Tips on how to protect yourself against cybercrime (2021) [online] kaspersky Available at: https://www.kaspersky.com/resource-center/threats/what-is-cybercrime (Accessed: 30 Nov 2021)

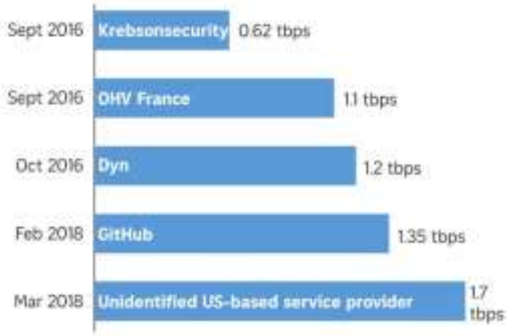
Varonis, 2021. 134 Cybersecurity Statistics and Trends for 2021[Online]. Available at: https://www.varonis.com/blog/cybersecurity-statistics/ (Accessed: 1 Dec 2021)

Verizon.com, 2019. 2019 Data Breach Investigations Report [online] Available at: https://www.verizon.com/business/resources/reports/2019-data-breach-investigations-report.pdf (Accessed: 29 Nov 2021]

Appendix

Cyber threats in 2018

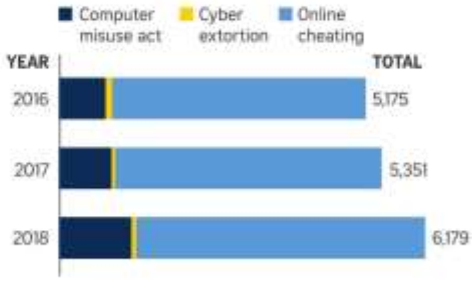
DDoS ATTACK PEAKS



Record peaks of distributed denial-of-service attacks - a comparison

In 2018, the largest Distributed Denial-of-Service (DDoS) attack ever recorded was conducted using a relatively new method. As threat factors find new attack methods, even higher peaks of DDoS attacks may be seen.

CYBERCRIME IN SINGAPORE



OVERVIEW OF
CYBER THREATS IN 2017
GLOBAL INCIDENTS
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
SINGAPORE INCIDENTS
PHISHING
23,420
2
1
3
WEBSITE DEFACEMENTS
2,040
MALWARE
750
2,700
>400
CYBERCRIME
5,430
RANSOMWARE
25
TYPES OF THREATS REPORTED TO SINGCERT*
11%
17%
21%