

Computer Law and Investigation

ST2502

Assignment: CA1

Class: DISM/FT/1B/04

|  |  |
| --- | --- |
| **Student Number** | **Full Name** |
| 1904189 | Lee Yi Terng |
| 1904291 | Sean Chye |
| 1950065 | Haziq bin Affendy |
| 1904361 | Lee Kah Boon |
| 1928864 | Lu Jia Jun |

Submitted to: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_

**Table of Contents**

[**Executive Summary**](#_nu4lvnmxxfyw)3

[**Issues on Computer Crimes**](#_ouci6nqpf0g9)4

[**Introduction**](#_t61tlw6w3p1d)4

[Introduction to computer crimes](#_hke1d51hpcor) 4

[Definition of computer crimes](#_jklu6ou4t1tk) 4

[**Background of Computer Crime**](#_a96gduohrdhu)4

[Some background knowledge of Computer Crime](#_b103rusmih91) 4

[**Types of Cyber Crimes**](#_kaidz4mne8u9)5

[Hacking](#_xjvj404rtsff) 5

[RansomWare](#_3jkuqi1g545u) 6

[Other Cyber Crimes](#_gunkgggi7arc) 6

[**Profile and Motivations of Computer Criminals**](#_hy283zillcus)7

[**Prevalence of Cyber Crime**](#_oq1m8zlq9wgw)8

[The commonness of computer crimes in recent years](#_t9ugt1wmzus8) 8

[From 2014 to 2016](#_wc3mn1b6fkx5) 8

[From 2017 to 2018](#_we5awftzwmax) 9

[Frequency of common attacks and examples](#_c72869wnki76) 9

[**Repercussions of Cyber Crime**](#_jklsxys3a1po)11

[Damage to the company’s image and productivity](#_u01gb3gbl95) 11

[Loss of information](#_h1uhcitmw1ji) 11

[Lawsuit and Legal Issues](#_3sgwnuvrn7ac) 12

[Personal Impacts](#_5opxkng23sbz) 13

[**Investigation**](#_p5n7m0ho2x2q)13

[Pre-Investigation](#_6zrj28yk4k02) 13

[Main Investigation](#_jugvyz1tscg) 14

[Post-Investigation](#_8i0upj65q3tf) 15

[**Conclusion**](#_r86wi3k770fy)15

[**References**](#_r8kpsgwb5kfb)16

# Executive Summary

Incidents of Computer Crime has surged in the past decade as technology continues to advance and become more accessible. Attackers have become more cunning and sophisticated with their attacks, leading to more people falling victim to various types of cybercrime. Companies and individuals alike have to keep up with the different attacks being used against them. “Threat is a mirror of security gaps. Cyber-threat is mainly a reflection of our weaknesses. An accurate vision of digital and behavioural gaps is crucial for a consistent cyber-resilience.” **-Stephane Nappo**

The types of cyber crime committed today are limitless, resulting in laws and security vendors struggling to come up with new solutions to deal with these acts of crime. “Hacking” is a very generic term to describe cybercrime, and that simple word sparks fear in the hearts of most common people.

The criminals who commit these acts come from various backgrounds and industries, with different skill sets and motivations. Cybercrime is no longer limited to just individuals with advanced knowledge of computer systems and networks. A simple script can easily be downloaded online from websites in order to launch an attack.

Laws have been implemented to protect us and it is the job of individuals and organisations alike to remain vigilant and follow standard operating procedures in order to ensure the safety and security of their online presence and digital information.

# 

# Issues on Computer Crimes

# Introduction

## Introduction to computer crimes

Computer crimes have become seemingly more ubiquitous throughout the decade. As mankind progresses further into the cyber age the tools used to infiltrate systems have also become more advanced. Threats have evolved from destroying physical property to cyberspace. Due to most of the world’s information being stored in files in cyberspace servers, computers and data centres are more vulnerable to attacks than ever before. To properly analyze the acts of computer crime, we first need to understand what is the meaning of computer crime and the laws that are passed to protect us.

## Definition of computer crimes

Computer crimes are defined as any harmful acts performed by any user with sufficient knowledge. Most commonly known as a ‘hacker’. They can work alone or in groups where they have ill motives such as stealing information, destroying data or corrupting computer files. Some examples are acts of Cyber Espionage, Harvesting, Identity theft.

# Background of Computer Crime

## Some background knowledge of Computer Crime

One of the earliest recorded cyber crimes happened in the 1820s. Joseph-Marie Jacquard, a textile manufacturer in France, developed the loom. This caused the employees of Jacquard to feel uneasy as they thought that the loom would prove superior traditional weaving and ultimately putting them out of their jobs. Therefore Jacquard’s employees sabotaged the development of the loom to discourage Jacquard from using it.

Computers have evolved from a simple abacus to advanced systems that can solve complex problems that even humans cannot comprehend, for example, the “Erdő discrepancy problem”

was thought to be too complex for a human to comprehend. The problem was finally solved by a computer after almost 6 decades. As computers evolve to be more capable and advanced, so do the cyberattacks created against them. These attacks are becoming more obscure and complicated than they were decades ago.

Computer crimes have also been on the rise, from 3.8 million breaches in 2010 to 3.1 billion breaches in 2016. The expected cost of cybercrimes is estimated to rise to 6 trillion US dollars in the coming years. “With an increase of more than 3 billion records breached over six years, cybercrime is rapidly increasing and it doesn’t seem like organisations’ security functions are keeping up”(Graham, 2019)

With Cyber Crimes being so flexible as data can be stored almost anywhere, there is a myriad of reasons that these crimes are committed. Some of which would include: Stealing of personal information and classified data to be sold on the black market or even online scamming to earn a quick buck.

# Types of Cyber Crimes

## Hacking

Hacking is usually regarded as an umbrella topic as it is very generic. This is the most well-known type of cybercrime. It has made headlines and cost a large amount of money in the destruction of both physical and digital properties. Hacking is generally defined as an act of gaining unauthorised access to data in a system or computer. One of the most infamous breaches of data happened recently in Singapore between 27th June 2018 and 4th July 2018. During that time, “SingHealth” was hacked, resulting in close to 1.5 million personal medical records being stolen and leaked, including the details of Singapore’s Prime Minister, Lee Hsien Loong.

## RansomWare

Ransomware is a malware that blocks user access to their files and requests for payment in real money or cryptocurrencies in return for access to the files. One popular example is called “WannaCry”, which caused about 4 billion US dollars in damage. WannaCry utilized the EternalBlue exploit which at that time was a secret kept by the US government, which caused infected systems to encrypt all user files, making it improbable for the user to retrieve their data. Being a Ransomware Cryptoworm, WannaCry was able to spread to 150000 computers worldwide causing damage ranging from hundreds of millions to billions of [dollars](https://en.wikipedia.org/wiki/United_States_dollar). It was ultimately resolved by updating the operating system of the infected machine. One of WannaCry’s vulnerabilities was that it was not programmed to improve itself and it only had the capability to attack legacy systems. Hence, a simple Windows System Patch could easily prevent the ransomware from infecting the system.

## Other Cyber Crimes

Cybercrime is a very broad topic; the types of cybercrime cannot be explained fully in this report. Other types of cybercrime include but are not limited to Fraud, Identity Theft, Scamming, Spreading of Viruses, Distributed Denial of Service (DDOS) attacks, Phishing, Botnets and Cyberstalking.

# 

# Profile and Motivations of Computer Criminals

Table 1: Characteristics, Techniques, and Targets of Cyber Threat Actors

|  |  |  |
| --- | --- | --- |
| **Cyber Threat Actors** | **Description** | **Motivation** |
| **Cyberterrorists** | Politically motivated attack on a nation’s network and computer infrastructure to cause disruption and panic among citizens. | Financial gain, power, cause panic, distrust in government. |
| **Hacktivists** | Attackers who attack for ideological reasons that are generally not as well-defined as a cyberterrorist’s motivation such as bringing awareness to a cause or disruption of a service they find unsatisfactory. | Ideological activism; disruption of services or access to information. |
| **Nation-State Actors** | An attacker commissioned by the governments to attack enemies’ information systems, very well resourced and well trained. | Advance the interests of their nation-state; further political agenda, high pay from the government. |
| **Cybercriminals** | Access personal, financial, or health data to monetize it. Moving from traditional criminal activities to more rewarding and less risky online attacks. | Financial gain; power. |

# Prevalence of Cyber Crime

## The commonness of computer crimes in recent years

### From 2014 to 2016

Cybercrimes nearly doubled in proportion between 2014 and 2016, rising from 7.9 to 13.7 percent of all crimes in Singapore. In a report released by the Cyber Security Agency of Singapore (CSA), it was found that 83 percent of all cybercrimes involved online cheating, followed by unauthorised access to computer material at 15 percent and cyber extortion at 2 percent. In 2016, 2512 phishing URLs were found and 1750 websites were defaced.

Offences under the Computer Misuse and Cybersecurity Act increased exponentially from 2014 to 2016, from 197 to 691 cases. Through studies, a trend was found, showing that criminals deviated towards ransomware, hacking, as well as undermining online accounts, including SingPass and Internet banking accounts. Another trend showed that victims of website defacements tended to be Small Medium Enterprises (SMEs). Roughly 10 percent of defaced websites were hosted on obsolete operating systems like Windows Server 2003, which no longer release new patches for vulnerabilities, making it simpler for hackers to exploit.

Online banking websites and websites for financial services were the most likely to be spoofed, making up 31 percent of phishing websites found in 2016. E-payment platforms such as PayPal and file-hosting services such as Dropbox and Google Drive were targets as well, and even government bodies such as the Ministry of Manpower and the Immigration and Checkpoints Authority were not spared. The CSA said threat actors wanted users’ personal data, for example, passport numbers and credit card numbers, which could be sold in illegal markets.

The top attack that affected SMEs is a form of phishing known as “business email scams”. Millions of dollars were lost through these scams, where attackers posed as white-collar workers or business partners through email. Such scams had increased by 20 percent between 2015 and 2016.

Additionally, over 60 Command and Control (C&C) servers were found in Singapore’s cyberspace in 2016. They were used to communicate with zombie computers and execute malicious attacks such as data theft, email spam campaigns and Distributed Denial of Services (DDoS) attacks, which involves overloading a system with spam requests, disrupting business operations and diverting defenders from other cybercrimes. Zombie computers are infected systems which allow an attacker to gain remote control of the computer to perform malicious actions.

### From 2017 to 2018

Common cyber threats were observed to have decreased in 2018 compared to 2017, though the number of cases of cybercrime continues to increase, with 6179 reported cases in 2018, making up 19 percent of the total crime in Singapore. Cases investigated under the Computer Misuse Act increased by around 40 percent since 2017, the number of which is now at 1204.

The most common type of attack is ransomware, which can be effectively spread through a watering hole attack, where a website is hacked and used to infect its visitors with malware, which majority of Singaporean businesses voted as the most destructive type of cybercrime.

## 

## 

## 

## 

## 

## Frequency of common attacks and examples

Table 2: frequency common attacks and examples:

|  |  |  |
| --- | --- | --- |
| **Type of attack** | **Frequency** | **Examples** |
| **Website defacements** | 605 web defacements were found in 2018, dropping from 2040 in 2017. | Main victims were SMEs, but larger enterprises, as well as 2 local government websites, were also compromised. In November 2018, 101 websites were hacked by the same person in a day due to unpatched vulnerabilities in a web server. |
| **Ransomware** | 21 ransomware cases were reported to CSA in 2018, a drop from 25 in 2017. | GandCrab, a rather invasive  ransomware, infected a private financial institution in Singapore through a “font update pack” that an employee downloaded to “view the website properly”. |
| **Phishing** | Phishing URLs with Singapore-links experienced a 30 percent drop, from 23420 URLs in 2017 to 16100 URLs in 2018. | Mainly banking companies, financial services, technology and file hosting services were spoofed. |
| **C&C Servers** | In 2018, about 300 unique C&C servers were found in Singapore (CSA), a 60 percent decrease from 2017. Almost 2900 botnet drones with Singaporean IP addresses were found daily and 470 malware variants were found. | Conficker, Mirai, WannaCry, Gamarue and Gamut accounted for more than half of the known infections. The commonness of such malware variants shows that many users have not adopted protective measures like patching their devices and using anti-viruses. |

# Repercussions of Cyber Crime

## Damage to the company’s image and productivity

When a company is hit with a cyberattack, they are forced to suspend all operations until the attack is dealt with. The time taken to repair the damage can span from days to weeks and even months depending on the severity of the damage caused. This will result in a loss in productivity due to time, money and resources spent on recovery instead of production.

Loss of revenue may not be the only issue to arise from cyber attacks. Damage to the reputation of businesses may be more severe than losing revenue as this would ruin any future endeavours such as bringing in new investors or promoting new products. If a customer’s personal data were to be leaked in a data breach, trust in the company would be lost as well.

## Loss of information

Loss of personal or sensitive information is another repercussion of cybercrime. Information is the lifeblood of any business and if their information is leaked or stolen there will be serious consequences that affect the business and those involved. An example is the aforementioned Singhealth data breach in 2018 where patients had their medical records stolen. Loss of information can also result in legal consequences, such as British Airways facing 183 million in fines after a data breach in 2018.

## Lawsuit and Legal Issues

Businesses that were victims of cyber-attacks are also subjected to lawsuits and legal issues. On 2nd March 2018, Singapore implemented the Cybersecurity Act,

* an Act to require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents.
* It is to regulate owners of critical information infrastructure, cybersecurity service providers, and for matters related thereto.
* It is also to make consequential or related amendments to certain other written laws, to ensure that businesses that own critical information infrastructure to follow the amendments.

A cyber-attack on businesses would trigger an investigation as stated in (19 and 20) of the Cybersecurity Act. If it is found that the reason for the successful attack was a result of negligence, the owner will be liable to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a continuing offence, to a further fine not exceeding $5,000 for every day or part of a day during which the offence continues after conviction. (Cybersecurity Act(12) )

Furthermore, businesses are also subjected to lawsuits from their clients, business partners and investors. For businesses that collect customers’ personal data, a lawsuit can be made against them under the Personal Data Protection Commission. An example of such would be Singhealth being sued $250000 as it was their responsibility to protect people’s personal information. The Integrated Health System (IHIS) was sued $750000 as they were responsible for creating the online infrastructure as well as securing the database.

## Personal Impacts

Businesses are not the only ones who suffer from cybercrime. Individuals are also affected as well. They can be scammed of their money through online scams such as product offers or “secret investment tricks” which turn out to be fake. Within the past year, cybercrime victims have lost almost $126 billion globally due to cybercrime. Passwords, credit card numbers and personal information can be stolen as well, which leads to severe consequences such as identity theft or data theft. Individuals have to take steps such as installing anti-virus software in order to ensure their safety and security in the digital world.

# 

# Investigation

## Pre-Investigation

For any computer crime investigation, a Computer Emergency Response Team (CERT) and a plan for conducting said investigation should already exist beforehand.

To start any investigation, the criminal action has to be detected first, either by accident or after reviewing audit trails. Once it is detected, the organization would have to minimize the risk of further loss in their systems by either shutting down their systems, rebooting their computers or running clean backups of their operating systems and programs.

Management would then be informed to take action to protect and preserve any potential evidence while the investigators begin their preliminary investigation. During the process, the investigators have to find out if a crime really did occur or if the incident was just an honest mistake. Once a crime is determined to have occurred, the company or organization will have to make various decisions on who should be informed, whether to disclose the incident, how much further they wish to investigate and such before the more detailed investigations can begin.

Once the decisions are made and official investigation can begin, a plan is drawn up to aide the investigators in their work. Some details would include the computer systems suspected to be used in the crime, risks of destruction of evidence and members of the investigating team. The investigation must also be covert, so as to not alert the culprit of it. Information of the case should only be relayed when necessary and not through any electronic device to prevent details from being leaked.

## Main Investigation

The first step to the investigation would be to secure and preserve the scene, which would be the network servers, telecommunication services and the power source. If the suspect is thought to be one of the workers, the suspect should be transferred to other positions that would not allow them to access those critical assets. When searching and seizing items to analyse, it is advised to do so after work hours to avoid people from finding out about the investigation. Though it may still be possible for the suspect to access the systems remotely through different systems like LAN-based or Internet connection, investigators would need to keep this in mind while analysing seized items.

When gathering evidence through the seized devices, investigators must not rush the process as that runs the risk of destroying evidence when they accidentally trigger malware like Logic Bombs which could impede their investigation. Investigators could video their investigation process to rebut any protests the suspect could have in court, though they should be careful of what they say and do since mistakes would be recorded into the video as well if they were careless. If the investigators do not wish to video the process, they need to take a picture of the crime scene with critical evidence present in them or sketch a drawn-to-scale image of the scene. The configurations of the computers or devices are extremely important. Documentation of each stage of the investigation must be made as well.

Evidence must be marked and packed properly after being identified. Evidence that can be considered or investigated during computer crime investigations includes LAN servers and routers, any forms of magnetic media like hard drives or floppy disks, hacker-tools and ill-gotten items like stolen credit card numbers, or other electronic devices that can store data like phones or fax machines.

Sometimes when surveillance of the target is required, investigators would check the CCTVs of the company or go undercover to learn about their suspect’s routine. Another surveillance method that would be used would be to monitor computer systems and their logs, investigators would require a warrant for this to prevent their evidence from being rejected and having charges placed on them. Investigators would also question witnesses for evidence or information that may be helpful to the investigation.

## Post-Investigation

Once the investigation is completed, investigators would need to make their reports. These reports should have an orderly and detailed sequence of information including a description of the incident, witness statements, evidence analysis, details of the crime scene and the conclusion of the investigation. Once the report is submitted, the defence and prosecutors will take over the case in court.

# Conclusion

Computer crime has been on the rise ever since we started using computers to store our information. Advancements in technology have created more complex and diverse cyber-attacks which makes our information more vulnerable than ever. There are ransomware attacks where our information is used against us and hackers gaining unauthorised access to our information and impersonate us, so we should be vigilant and learn how to protect our own information. Should any business fall victim to a cyberattack the consequences would be severe. Take for example the Singhealth data breach; it caused them to be sued for $250,000 and caused fear and unrest in the community. To counter the cybercrimes, Singapore established the Cybersecurity Act (CSA) and the Computer Misuse Act (CMA), but even with these new laws, Singapore continues to a target of advanced threat actors.

# 

# 

# 

# 

# 

# References

Available at

https://sso.agc.gov.sg/Acts-Supp/9-2018/

[Access 20 Nov 2019]

Welch, T. (n.d.). *Computer Crime Investigation and Computer Forensics*. [ebook] Auerbach Publications, pp.11-27. Available at: http://www.ittoday.info/AIMS/DSM/82-30-25.pdf [Accessed 23 Nov. 2019].

Irene, Tham. (2019) *Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach.* [online]. Available athttps://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach

[Access 20 Nov 2019]

Cyber Security Agency. (2019). *CSA | Fewer Cases of Common Cyber Threats Detected in Singapore in 2018*. [online] Available at: https://www.csa.gov.sg/news/press-releases/fewer-cases-of-common-cyber-threats-detected-in-singapore-in-2018 [Accessed 20 Nov. 2019].

Cyber Security Agency. (2019). *CSA | Fewer Cases of Common Cyber Threats Detected in Singapore in 2018*. [online] Available at: https://www.csa.gov.sg/news/press-releases/fewer-cases-of-common-cyber-threats-detected-in-singapore-in-2018 [Accessed 25 Nov. 2019].

Koh, S. (2019). *Proportion of cyber crimes in Singapore growing*. [online] TODAYonline. Available at: https://www.todayonline.com/singapore-proportion-cyber-crimes-growing [Accessed 25 Nov. 2019].

Singh, N. (2019). *Singapore is One of the World's Tech Leaders, Yet its Companies Are Struggling to Fight Cyberattacks*. [online] Entrepreneur. Available at: https://www.entrepreneur.com/article/332009 [Accessed 18 Nov. 2019].