Computer Misuse Act

Computer Misuse Act (Chapter 50A)

Computer Misuse Act, was enacted in 1992 to address computer crimes in Singapore. An amendment was later introduced in Parliament in 1998. The new Amended Act supposedly is to take a more sophisticated approach to provide for enhanced penalties proportionate to the different levels of potential and actual harm caused. [1105sgict:4]

1. Types of Crimes

The Computer Misuse Act covers offences for several computer crimes. Some of which includes unauthorised access to computer materials, access with intent to commit or facilitate commission of offence, modification of computer material, use or interception of a computer service, obstruction of the use of a computer and disclosure of access code. [1105sgict:6]:


1.1 What is "computer crime" and what is "cyber crime"?

To clarify, the term 'computer crime' is different from 'cyber crime'. Computer crime involves acts that attack the functions of a computer, access to a computer or the Internet, etc. This can be likened to property trespassing. Examples of these crimes are hacking, denying another access to Internet usage, and sending unsolicited or virus-causing electronic mail.

On the other hand, cyber crimes are crimes committed in cyberspace but in this case the computer is used as an instrument of carrying out the crime. Examples include, fraud, theft, and extortion. (2)

2. Offences/Liabilities

2.1 Unauthorised access to computer material

Unauthorised access to computer materials refers to 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. (1)

Some examples include: using another person's identifier (ID) and password without proper authority in order to use data or a program, or to alter, delete, copy or move a program or data, or simply to output a program or data.

2.1.1 Penalty

Offender shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both.[1105sgict:1]

If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both.[1105sgict:1]

2.2 Access with intent to commit or facilitate commission of offence

This refers to 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.

Some examples include: online offences involving property, fraud, dishonesty such as gaining access to financial or administrative records and manipulating banking system to commit identity theft. However, the court would have to prove the intent of the offender.

2.2.1 Penalty

Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both.[1105sgict:1]

2.3 Unauthorised modification of computer material

This refers to any person who does and is aware of making any unauthorised modification of the contents of any computer.

Some examples include: destroying another user's files; modifying system files; creation of a virus; introduction of a local virus; introduction of a networked virus; changing examination results; and deliberately generating information to cause a complete system malfunction.

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

If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both. [1105sgict:1]

2.4 Unauthorised use or interception of computer service

This refers to any person who knowingly and without authority: (i) secures access to any computer to obtain services; or (ii) intercepts, records or listens to a function or a communication to or from a computer; or (iii) uses any other device to carry out acts. [1105sgict:6]

Some examples include: Hacking of computer systems for the purpose of gaining free internet services or to carry out spying activities. [1105sgict:6] Hacking includes a wide range of activities such as monitoring, thievery, exploitation, altering, vandalism, and destruction of computer systems, all of which endanger individuals’ rights to privacy and security. The hacking process is performed by a hacker, a person that uses programming skills to gain illegal access to a computer, a network or a file. [1105sgict:5]

2.4.1 Penalty

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

If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both. [1105sgict:1]

2.5 Unauthorised obstruction of use of computer

This refers to any person who, knowingly and without authority or lawful excuse: (i) interferes, interrupts or obstructs the use of a computer; or (ii) impedes or prevent access to, or impairs the usefulness or effectiveness of a program or data stored in a computer. [1105sgict:1]

One example includes email bombing, which is characterized by abusers repeatedly sending an email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact. [1105sgict:3]

2.5.1 Penalty

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

If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both. [1105sgict:1]

2.6 Unauthorised disclosure of access code

This refers to disclosing one’s access code to any program or data held in any computer and the disclosure was for a wrongful gain, unlawful purpose or with the knowledge that it is likely to cause wrongful loss to any person. [1105sgict:6]

One example includes sale of one’s company’s access code to confidential information to others.

2.6.1 Penalty

Any person guilty of the offence shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. [1105sgict:1]

2.7 Enhanced punishment for offences involving protected computers

This refers to the situation where access to any protected computer is obtained in the course of the commission of an offence under section “Unauthorised access to computer material”, “Unauthorised modification of computer material”, “Unauthorised use or interception of computer service” or “Unauthorised obstruction of use of computer”. [1105sgict:6]

2.7.1 Penalty

Offender 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. [1105sgict:1]

3. What else has been done?
Singapore has also created new law enforcement agencies with specially trained personnel to keep pace with the rapid advances in technology and the resulting proliferation of computer-based crimes. It has given its police force additional powers, including extra-territorial jurisdiction to aid in their efforts at apprehending computer-based criminals. [1105sgict:2]

4. Reference


