Chapter 5 LEGAL MATTERS

Despite its sophistication and complexities, ICT systems are vulnerable to abuse and threats. This may result in damage such as loss of confidentiality, information integrity, authenticity, availability, etc. Examples of threats to ICT environments are as listed in Appendix B.

Importance of cyber laws.

Cyber laws form an important component of the legal framework needed to facilitate the development of ICT systems by countering the threats and abuses related to such systems.

Cyber laws in response to ICT security requirements.

In relation to ICT security, cyber laws were enacted to:

(a) regulate and protect the ICT industry from misuse and illegal activities or activities that assist in the commissioning of illegal activities. Above all, cyber laws seek to promote the development of local ICT-based industries;

(b) describe in clear terms activities construed under the law as offences;

(c) describe in detail penalties for transgression; and

(d) provide soft infrastructure to lend support to the MSC initiative.

No.	***Act***	***Date of Royal Assent***	***Date of Publication in Gazette***	***Date of Enforcement***
1.	Digital Signature Act 1997	June 18, 1997	June 30, 1997	October 1, 1998
2.	Computer Crime Act 1997	June 18, 1997	June 30, 1997	June 1, 2000
3.	Telemedicine Act 1997	June 18, 1997	June 30, 1997	*
4.	Copyright (Amendment) Act 1997	June 18, 1997	June 30, 1997	April 1, 1999
5.	Communications & Multimedia Act 1998	September 23, 1998	October 15, 1998	April 1, 1999
6.	Malaysian Communications & Multimedia Commission Act 1998	September 23, 1998	October 15, 1998	April 1, 1999

* To be enforced

Table 5.1: Malaysian Cyber Laws

Other regulations related to computer crime.

In addition other existing regulations, which are related to computer crime include:

(a) Copyright Act 1987;

(b) Official Secrets Act 1972;

(c) Companies Act 1965 (Act 125);

(d) Trade Marks Act 1976;

(e) Patents Act 1983;

(f) Prison Act 1995; and

(g) Akta Arkib Negara 44/1996.

5.1 Cyber Laws and Legal Implications

5.1.1 Digital Signature Act 1997

Provision of the Digital Signature Act.

The Digital Signature Act was enacted to instill confidence and encourage the public to perform secured electronic transactions domestically as well as internationally. Under the Act, the digital signature provides a verification system to authenticate the identity of the author and verify the transmitted message.

Certificate must be obtained from Certification Authority.

For a digital signature to be recognised, it is necessary to obtain a certificate from a Certification Authority licensed by the Controller of Certification Authorities. On the salient elements of this law are that Certification Authorities authorised by a foreign government entity may be recognised and that the liability of a Certification Authority is limited. A document created in accordance with this Act or signed digitally is legally binding as a document.

Among the provisions of this Act are:

(a) the need for all Certification Authorities to be licensed;

(b) the appointment of a Controller of Certification Authorities;

(c) the main responsibility of a Controller of Certification Authorities is to license the Certification Authority;

(d) the main task of the Certification Authority is to verify the identity of subscribers;

(e) determination of the liability limits of the Certification Authorities and the legal effect of digital signatures; and

(f) delegation of authority to the Minister to appoint the Controller of Certification Authority.

5.1.2 Computer Crime Act 1997

Provision of Computer Crime Act.

The Computer Crime Act 1997 relates to offences due to the misuse of computers and complement existing criminal legislation. Under this law, unauthorised access/modification to any programme or data held in computer is an offence and will be penalised. This Act also has an effect outside Malaysia if the offences are committed by any person in any place outside Malaysia if the computer, programme or data is in Malaysia or capable of being connected to or used with a computer in Malaysia.

An abstract of the offences, punishment and enforcement under the Act are listed below:

List of Offences

Section	*Offences*
3	Unauthorised access to computer material
4	Unauthorised access with intent to commit or facilitate commission of further offence
5	Unauthorised modification of the contents of any computer
6	Wrongful communication
7	Abetments and attempts punishable as offences
8	Presumption
11	Obstruction of search

List of Punishment

Section	*Imprisonment*	*Fine*	*Or Both*
3	Not > 5 years	Not > RM 50,000.00	✓
4	Not > 10 years	Not > RM 150,000.00	✓
5	Not > 7 years; If cause injury, not > 10 years	Not > RM 100,000.00; If cause injury, Not > RM 150,000.00	✓
6	Not > 3 years	Not > RM 25,000.00	✓
7	Not > 1/2 of maximum term	Same amount as offences abetted	✓
11	Not > 3 years	Not > RM 25,000.00	✓

List of Enforcement

Section	*Offences*	*Search & Seizure*	*Arrest*
10	Powers of search, seizure & arrest	Person: not less than Inspector With or without warrant	Person: Any Police Officer. Without warrant (Seizable)

Table 5.2: List of Offences, Punishment and Enforcement

5.1.3 Telemedicine Act 1997

Provision of the Telemedicine Act.

The Telemedicine Act was enacted to provide the regulatory framework for the practice of Telemedicine and to recognise the use of multimedia in the practice of medicine.

Telemedicine can be practiced by a licensed personnel.

Telemedicine can be practiced by a local doctor who has a valid practicing certificate, a foreign licensed/registered doctor who has been certified by the Malaysian Medical Council through a local doctor or provisionally registered medical practitioner, medical assistant, nurse and midwife approved by the Director-General of Health. No other person can practice Telemedicine and offenders will be fined accordingly. The important condition in telemedicine is that the doctor must obtain written consent from the patient for such treatments. However, there is no provision in the Telemedicine Act on the liability of telemedicine practitioners. Liability is to be determined by tortuous or contractual principles.

Provision of Copyright (Amendment) Act.

5.1.4 Copyright (Amendment) Act 1997

This Act is to enhance copyright protection by taking into account development in information technology and the latest developments related to copyright under the World Intellectual Property Ownership (WIPO) Copyright Treaty 1996. The scope of copyright protection has been widened where an author is also given exclusive right of control. New copyright infringements and offences have been further identified and regulated under this Act.

An abstract of the offences, punishment and enforcement under the Act are listed below:

List of Offences

Section	***Offences***
41(1)(h)	Circumvents or causes the circumvention of any effective technological measures referred to in S.36 (3)
41(1)(i)	Removes or alters any electronic rights management information without authority
41(1)(j)	Distributes, imports for distribution or communicates to the public, without authority, works or copies of works in respect of which electronic rights management information has been removed or altered without authority

List of Punishment

Section	*Imprisonment*	*Fine (RM)*	*Or Both*
41(1)(h)	Not > 3 years Subsequent offence not > 5 years	Not > RM 250,000.00, Subsequent offence not > RM 500,000.00	✔
41(1)(i)	Not > 3 years Subsequent offence not > 5 years	Not > RM 250,000.00 Subsequent offence not > 500,000.00	✔
41(1)(j)	Not > 3 years; Subsequent Offence not > 5 years	Not > RM 250,000.00; Subsequent offence not RM 500,000.00	✔

List of Enforcement

Section	*Offences*	*Investigation*	*Search & Seizure*	*Arrest*
44	Entry by warrant or otherwise	-	Police not less than Inspector or Assistant Controller	-
50	Power of investigation	Police not less than Inspector or Assistant Controller	-	(Special power investigation) Police -without warrant Assistant Controller - with warrant

Table 5.3: List of Offences, Punishment and Enforcement

5.1.5 Communications and Multimedia Act 1998

Provision of the Communication and Multimedia Act.

This Act covers communications over the electronic media (exclusion of print media) and does not affect the application of existing laws on national security, illegal content, defamation and copyright. This Act, regulates various activities such as network facilities providers, network service providers, application service providers and content application services providers. Under this Act, the Minister is given the flexibility to grant licences for particular types of activity as he deems fit. This flexibility is to address of the changing requirements as the industry evolves.

5.1.6 Malaysian Communications & Multimedia Commission Act 1998

Provision of the Malaysian Communications and Multimedia Commission Act.

This Act provides the establishment of the Malaysian Communications and Multimedia Commission with powers to supervise and regulate the communications and multimedia activities in Malaysia, to enforce the communications and multimedia laws of Malaysia, and for related matters.

5.2 Crime Investigation

Increasing ICT security incidents.

Global trends indicate that ICT security incidents (fraud, theft, impersonation, loss of business opportunity, etc.) are increasing.

This is primarily due to:

(a) readily available facilities and tools plus the lack of control in their use;

(b) relatively easy in mounting attacks from a distance; and

(c) availability of valuable information on networks that could be exploited.

It is imperative that public sector officers involved in ICT security are aware of such incidents so as to enable them to mitigate risk and exposure of their respective ICT installations, including issues dealing with investigations and enforcement.

Few convictions due to grey areas.

Telecommunications fraud, computer-related crime incidents, investigations and computer forensics involve sciences affected by many external factors, such as continued advancements in technology, societal issues and legal issues. Most of the cases are esoteric in nature and there have been very few prosecutions and even fewer convictions being made. This is because of the many grey areas to be sorted out and tested through the courts. Until then, system attackers will have an advantage and computer abuse will continue to increase.

5.2.1 Definition of Computer Crime

Computer crime is a criminal act.

Computer crime is defined by the Royal Malaysian Police as:

(a) a criminal act in which a computer is **essential** to the perpetration of the crime; or

(b) a criminal act where a computer, **non-essential** to the perpetration of the crime, acts as a store of information concerning the crime.

5.2.1.1 Examples of Computer Essentials

Examples of computer essentials.

Some examples of computer essentials are:

(a) information theft via hacking;

(b) electronic funds transfer fraud;

(c) distribution of pornography via Internet;

(d) internet cash fraud; and

(e) credit card fraud.

5.2.1.2 Examples of Computer Non-Essentials

Examples of computer non-essential.

Some examples of computer non-essentials are:

(a) all types of fraud;

(b) murder;

(c) theft;

(d) forgery; and

(e) potentially any type of crime.

5.2.2 Evidence

Computer related crime evidence is intangible and may differ from traditional forms.

Evidence is defined as anything offered in court to prove the truth or falsity of a fact in issue. However, evidence presented in a computer-related crime case may differ from traditional forms of evidence because in most cases the computer-related crime evidence is intangible. As a consequence, the legal problems of computer-based evidence are intensified and complex.

5.2.2.1 Types of Evidence

Different type of computer related crime evidence.

The most common forms of evidence that can be offered in court to prove the truth or falsity of a given fact are:

(a) direct evidence is oral testimony obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue (e.g., an eyewitness statement);

(b) real evidence also known as associative or physical evidence. It is made up of any tangible objects that prove or disprove guilt;

(c) documentary evidence is evidence presented in the form of e.g. business records, manuals, and printouts. Much of the evidence submitted in a computer crime case is documentary evidence;

(d) demonstrative evidence is evidence in the form of a model, experiment, chart, or an illustration offered as proof;

(e) physical evidence includes tools used in the crime, fruits of the crime, or perishable evidence capable of reproduction to link the suspect to the crime; and

(f) computer generated evidence such as:

i. visual output on the monitor;

ii. printed evidence on a printer/plotter;

iii. film recorder (i.e., a magnetic representation on disk and optical representation on CD); and

iv. data and information stored electronically on storage devices (e.g. diskettes, CD's, tapes, cartridges etc.).

5.2.3 Conducting Computer Crime Investigation

Immediately start the investigation after the report is made.

The computer crime investigation should start immediately following the report of any alleged transgression or criminal activity. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process.

5.2.3.1 Detection and Containment

Steps to be followed before the investigation.

Before any investigation, the following steps should be taken:

(a) the system intrusion or abusive conduct must first be detected. Swift detection of the actual intrusion not only helps to minimise system damage, but also assists in the identification of potential suspects;

(b) proactive and automated detection techniques must be instituted to minimise the amount of system damage in the wake of an attack; and

(c) once an incident is detected, it is essential to minimise the risk of any further loss by shutting down the system and reloading clean copies of the operating system and application programmes. However, failure to contain a known situation (i.e. a system penetration) may result in increased liability for the victim's organisation.

5.2.3.2 Report to Management

ICT incidents should be reported to the management immediately

All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible. Information should be given on a need-to-know basis, which limits the possibility of the investigation being leaked. E-mail should not be used to discuss the investigation on a compromised system.

Also, ICT incidents should be reported to the relevant parties.

Based on the type of crime and type of organisation it may be necessary to notify:

(a) CIO;

(b) MAMPU;

(c) The Office of the Government Chief Security Officer, Prime Minister's Department;

(d) The Audit Department, Prime Minister's Department;

(e) The Legal Affairs Division, Prime Minister's Department; and

(f) The Attorney-General's Department, Prime Minister's Department.

5.2.3.3 The Preliminary Investigation

Preliminary investigation proses

The preliminary investigation usually involves the following:

(a) a review of the initial complaint, inspection of the alleged damage or abuse, witness interviews, and, finally, examination of the system logs;

(b) the investigator must address the basic elements of the crime to determine the chances of successfully prosecuting a suspect either via civil or criminal action;

(c) the investigator must identify the requirements of the investigation (i.e., the financial implication and resources); and

(d) the investigator should not confront or talk with the suspect. Doing so would only give the suspect the opportunity to hide or destroy evidence.

5.2.3.4 Determine if Disclosure is Required

Determine if disclosure is required

It is important to determine if a disclosure is required or warranted under specific laws or regulations. Even if disclosure is not required, it is sometimes better to disclose the attack to possibly deter future attacks.

5.2.3.5 Investigation Considerations

Factors to consider when deciding to further investigate

There are many factors to consider when deciding whether to further investigate an alleged computer crime.

The investigation considerations are:

(a) the cost associated with an investigation;

(b) the effect on operations or the effect on the organisation's reputation; and

(c) the victim organisation must answer these questions:

i. will productivity be stifled by the inquiry process?;

ii. will the compromised system have to be shut down to conduct an examination of the evidence or crime scene?;

iii. will any of the system components be held as evidence?;

iv. will proprietary data be subject to disclosure?;

v. will there be any increased exposure for failing to meet a 'standard of due care?';

vi. will there be any potential adverse publicity related to the loss?; and

vii. will a disclosure invite other perpetrators to commit similar acts, or will an investigation and subsequent prosecution deter future attacks?.

5.2.3.6 Who Should Conduct the Investigation?

Based on the type of investigation (i.e., civil, criminal, or insurance) and extent of the abuse, the victim must decide who is to conduct the investigation.

Victim is able to decide on the conducting party

The victim must choose from these options:

(a) conduct an internal investigation;

(b) bring in MAMPU to assess the damage, preserve evidence and provide recommendation for further action (refer to Appendix H: *Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)*); and

(c) bring in law enforcement officials.

Issue affecting are information dissemination, investigation control, cost and legality

The major issues affecting the decision as to which parties to bring (in order of priority) are information dissemination, investigative control, cost, and the associated legal issues. Once an incident is reported to law enforcement, information dissemination becomes uncontrolled. Law enforcement controls the entire investigation, from beginning to end. This does not always have a negative effect, but the victim organisation may have a different set of priorities.

Cost is of concern to conduct the investigation.

Cost is always a concern, and the investigation costs only add to the loss initially sustained by the attack or abuse. Even law enforcement agencies, which are normally considered “free”, add to the costs because of the technical assistance that they require during the investigation.

There are advantages and disadvantages for each of these groups previously identified. Internal investigators know the victim’s systems best, but may lack some of the legal and forensic training. Private investigators who specialise in high-technology crime also have a number of advantages, but usually involve higher costs. Private security practitioners and private investigators are also private businesses and may be more sensitive to business resumption than law enforcement.

Police involvement.

If the victim organisation decides to report to the police, care must be taken not to alert the perpetrator. When a police report is made the incident will become part of a public record. Now, there will no longer be on avenue for discretionary dissemination of information or a covert investigation. Therefore it is suggested that the victim organisation should ask the police to meet with it in plainclothes. When they arrive at the workplace, they should be announced as consultants. Be aware that the local law enforcement agency may not be well equipped to handle high-tech crime. Usually local law enforcement has limited budgets and place emphasis on problems related to violent crime and drugs. Moreover, with technology changing so rapidly, most local law enforcement officers lack the technical training to adequately investigate an alleged intrusion.

The same problems hold true for the prosecution and the judiciary. In order to prosecute a case successfully, both the prosecutor and the judge must have a reasonable understanding of high-technology laws and the crime in question, which is not always the case. Moreover, many of the current laws are woefully inadequate. Even though an action may be morally and ethically wrong, it is still possible that no law is violated (e.g., the LaMacchia case). Even when a law that has been violated, many of these laws remain untested and lack precedence. Because of this, many prosecutors are reluctant to prosecute high-technology crime cases.

Some of the defences have been used and accepted.

Some of the lines of defences that have been used, and accepted by the judiciary, are:

(a) if an organisation has no system security or lax system security, that organisation is implying that no organisation concern exists. Thus, there should be no court concern;

(b) if a person is not informed that access is unauthorised, it can be used as a defence; and

(c) if employees are not briefed and do not acknowledge understanding of policy, standards and procedures, they can use it as a defence.