THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 2 Article 1

2007

Computer Crimes: A Case Study of What Malaysia Can Learn from Others?

Janaletchumi Appudurai
Department of Business Studies, HELP University College

Chitra L. Ramalingam
Department of Business Studies, HELP University College

Recommended Citation

Appudurai, Janaletchumi and Ramalingam, Chitra L. (2007) "Computer Crimes: A Case Study of What Malaysia Can Learn from Others?," *Journal of Digital Forensics, Security and Law*: Vol. 2 : No. 2 , Article 1.
DOI: https://doi.org/10.15394/jdfsl.2007.1020
Available at: https://commons.erau.edu/jdfsl/vol2/iss2/1

Computer Crimes: A Case Study of What Malaysia Can Learn from Others?

Janaletchumi Appudurai
Department of Business Studies
HELP University College
e-mail: janaletk@help.edu.my

Chitra Latha Ramalingam
Department of Business Studies
HELP University College
e-mail: chithlr@help.edu.my

ABSTRACT

Rapid development of information technology (IT) has brought with it many new applications such as e-commerce and global business. The past few years have seen activities in the legislative arena covering issues such as digital signatures, the international recognition of electronic documents and privacy and data protection. Both the developed and developing countries have exhibited keenness to embrace the IT environment. Securing this electronic environment from intrusion, however, continues to be problematic. A particular favorite form of computer crime would be 'hacking'. As more computer systems move on to on-line processing and improved telecommunications, computer hackers are now a real threat. Legislation criminalizing intrusion and destruction activities directed at computers are needed. Malaysia joined the list of countries with computer-specific legislation with the enactment of its Computer Crime Act 1997 (CCA). This paper focuses on hacking as a criminal act, and compares the Malaysian CCA with legislation from other countries. The current computer crime situation in Malaysia is looked at and exposes the difficulties and obstacles Malaysia faces in enforcing the Act. The paper concludes with recommendations for Malaysia in terms of policy, practices and penalties.

Keywords: computer crime, computer hacking, hackers, Computer Crime Act 1997, Malaysia, Singapore, United Kingdom and United States of America.

1. INTRODUCTION

Rapid development of information technology (IT) has brought with it many new applications and opportunities. In the past few years, many activities in the legislative arena have taken place, covering issues such as digital signatures and the recognition of electronic documents internationally.

Whilst adopting IT and its application can be straightforward, securing this

electronic environment from hacking, however, continues to be a problematic issue (Eschelbeck, 2000). This can be seen from reports on hacking attacks (Masden, 1998) and the frequent requests by law enforcement for more resources to handle computer crime. Legislation often lags behind (Hull, 2000).

Many governments worldwide have come up with specific legislation criminalizing hacking. Malaysia joined the list of countries with computer specific legislation with the enactment of its Computer Crimes Act 1997 (Annamalai, 1997). The Act deals with unauthorized access to computer material, unauthorized access with intent to commit other offences and unauthorized modification of computer intent. It also makes the provision to facilitate investigation. In certain circumstances, the Act has extra territorial effects (The Computer Crime Act 1997).

This paper examines Malaysia's CCA 1997, to understand the basis of policy that gives powers of investigation and sets penalties in computer crime legislation. The Malaysian legislation will be compared with that from other countries. The paper will seek to answer several questions: What is the current computer crime situation in Malaysia? Is Malaysia enforcing its CCA 1997, and what are the difficulties? What can Malaysia learn from other countries in order to amend or fine tune the CCA 1997? The paper focuses on violations that deal with hacking and unauthorized access to computer-based information systems.

2. COMPUTER CRIME AND HACKING

The term *computer crime* now appears in the legislation of many countries (Edappagath, 2004). Countries are giving computer crimes special attention within their Internet regulations. Computer crimes comprise two overlapping domains. The first one is illegal activities directed at or perpetrated through the use of the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism. The second area is the protection of *information*, which include amongst others several legal measures related to the protection of information from unlawful use and distribution which include intellectual property laws, privacy laws, data protection law and others. Since this paper is only concerned with intrusion and illegal access to computer systems, this discussion will focus on *hacking*.

Hackers access computer networks, without authorization, to read, copy, alter, or destroy information (Zeng, & Hamzah, 2005). Hacking is basically a procedure in which more computer savvy individuals are able to penetrate the security system of the computer systems of individuals and corporations to steal data and information and to activate certain files for their own purposes, or to plant viruses or Trojan Horses (Hamzah, Z. 2005). From the point of view of the hackers, however, hacking is '*gaining knowledge about computers and security'* or *'self-teaching about computers and security'* (Granger, 1994).

Many hackers promote *'hacker ethics'*, which is a belief that essentially all information should be open and available (Hamzah, 2005).

Indeed, hacking is a very complicated ethical and legal issue that causes problems regarding the creation of laws and the enforcement of policies. Hackers, may be driven by greed, power, revenge, adventure and the desire to be able to penetrate a secured system. It can also be ideologically motivated, as when someone attacks the web site of religious or political groups to erase or change their content, therein entailing an element of a dangerous adventure. The fact that these destructive activities will bring official condemnation is often sufficient to attract the defiant, the rebellious, or the curious (Grabosky, 2001).

An example of hacking attack is *Denial of Service* (Yang, 2001), a crime that is unique to computer systems. In February 2000, a number of targeted sites which included amongst others, *Amazon.com*, *Yahoo.com*, and *CNN.com* (CNN, 2000), who were flooded with phony connection requests. Bogged down by efforts to handle all the requests, these sites slowed to a crawl or crashed.

The global nature of cyberspace significantly enhances the ability of offenders to commit crimes in one country, affecting individuals in other countries as well. This poses challenges for the detection, investigation, and prosecution of offenders (Grabosky, 2001). As for the prevention of such attacks, a number of fixes have been proposed (Bellouin, 2001), including encryption and firewalls. Despite all these efforts, computers are still being hacked. Why haven't these solutions worked? Hackers have ways to overcome these solutions and come out with new methods of breaking into systems. Certainly computers will still face threats with the emergence of new technologies (Posch, 2001). Detecting an intrusion is a first step in defending against a hacking attack (Durst *et. al* 1999).

3. MALAYSIA AND COMPUTER HACKING

In Malaysia as elsewhere, there has been an increase in the number of Internet Providers (IPs), and in the number of users. Within a population of 27.4 million in the year 2006, (Malaysian Statistics Dept., 2006), there are about 11.0 million Internet users in Malaysia today (Malaysian Statistics Dept., 2006). The growth of the Internet has meant more windows of opportunities for computer crimes. To anticipate such abuses, the Malaysian Parliament has passed several pieces of cyber related legislation since 1997.

Hacking is an increasing problem in Malaysia, even though it is done progressively in small doses. In June 2000, a vandal calling himself *'Xenophoria'* attacked 21 pro government web sites, posting a list of demands for greater press freedom and an end to corruption (USA Today, 2000). Thereafter, in the early year of 2001, a vandal calling himself *'Topeira'* hacked

the official web site belonging to the Parliament and University Teknologi Malaysia (UITM). It was alleged that this could have been in response to the Malaysian Government's announcement that it is establishing a special IT security lab and task force (ZDNetAsia, 2001). According to the National ICT Security and Emergency Response Centre of Malaysia (NISER), 899 information and technology intrusions were reported between the months of January to December 2006 (NISER, 2006). According to NISER, the number of computer intrusions for the period of the year 2006 had increased by 100 per cent compared to the year of 2005 (NISER, 2006). Statistics may show the trend on hacking crime activities, but they are not the reliable source to determine the actual position of the computer hacking rate. Criminologists use the term '*dark figure'* to describe the undetermined actual position which refers to those undetected computer hacking activities. Several contributing factors below may explain why it is called the *'dark figure'* (NISER, 2004).

First, the fast operational speed of today's computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity. Third, once criminal activity has been detected, many businesses are reluctant to lodge a report due to fear of adverse publicity, loss of goodwill, embarrassment, loss of public confidence, investor loss, or economic repercussions (NISER, 2004).

4. COMPUTER CRIME ACT 1997 (CCA)

Malaysia Computer Crime Act 1997 (Annamalai, 1997) has been drafted to provide offenses relating to the misuse of computers and to complement existing criminal laws. 'Hacking' or 'computer crime' is not defined in the CCA, but the word used is 'unauthorized access to computer material'. Section 3(1) provides that a person shall be guilty of an offence if –

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorized; and

(c) he knows at the time when he causes the computer to perform the function that is the case.

Persons found convicted of an offense within the proviso of Section 3 are liable to a fine not exceeding RM50,000 or to imprisonment not exceeding five years or to both (S. 4(1)(a) MCCA). Additional penalty is imposed if unauthorized access was used to commit or facilitate the commission of an offense involving fraud, dishonesty or which caused injury as defined by the Penal Code, (S. 4(1)(a) MCCA). The commission of the offense referred to need not be at the same time as the unauthorized entry. Persons convicted of an offense under section 4 are liable to a fine not exceeding RM50,000 or to imprisonment not exceeding 10 years or to both.

Section 2(2) states that a person secure access to any programme or data held in a computer if, by causing a computer to perform any function, he –

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d) causes it to be output from the computer in which it is held whether by having it displayed or in any other manner.

Section 2(5) further clarifies that access of any kind by any person to any program or data held in a computer is unauthorized if –

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have the consent or exceeds any right or consent to access by him of the kind in question to the program or data from any person who is so entitled.

The CCA also makes it an offence if a person does any act which he knows will cause unauthorized modification of the contents of any computer, Section 5(1). Section 6(1) makes it an offence for a person to communicate directly or indirectly a number, code, password or other means of access to a computer to any person other than a person to whom he is duly authorized to communicate. The CCA also seeks to make the offence extra-territorial in scope when it provides by Section 9(1) that the provisions of the CCA shall, in relation to any person, whatever his nationality or citizenship, have effect outside as well as within Malaysia, and where an offence under the CCA is committed by any person in any place outside Malaysia, he may be dealt with in respect of such offence as if communicated at any place within Malaysia.

A common sense reading, however, will imply that there must be at least some connection to Malaysia before the court can claim any jurisdiction to try the act as an offence under the CCA. Many such laws have been rather ineffective because of the difficulty in obtaining evidence due to the nature of the Internet and the ease in faking identities and even locations. There is also a problem due to the lack of resources and technical understanding by the judges and the police force.

The above was amplified in one instance, when a case collapsed because the police were unable to show the chain of evidence where a particular computer was concerned. The computer did not remain in the possession of the police for the entirety of the investigation. Therefore the computer may have been tampered with an evidence could have been altered (KPMG, 2005).

The nature of *'evidence'* for a successful prosecution of the new hacking

offences can be a problem for the enforcement agencies. In all cases of computer intrusion, the target computer's electronic log files and audit trails are crucial and sometime the only indication of intrusion. However, due to the nature of electronic data, the operators of the target server or even the hacker himself are in the position to modify and change the content of the log files, before, during and after the intrusion process (Hamzah, 2005). As such the accuracy or the integrity of the log files and other similar data can be compromised and cannot be guaranteed. Some experts have even suggested that due to its vulnerability to manipulation such logs should not be admissible as evidence in the court (Nair, 1997). Therefore deletion of the log files may make it difficult for the prosecution to prove its case beyond reasonable doubt.

5. COMPUTER CRIME LAWS IN OTHER COUNTRIES

In this section, I will analyze the current state of computer crimes across three continents – Singapore, the United Kingdom and the United States. The respective laws of these countries will be discussed for the purpose of comparison and reflection on the CCA.

5.1. United Kingdom (UK) Computer Misuse Act 1990

The UK computer crimes legislation is the Computer Misuse Act of 1990 (CMA) (website of UK govt.). Government departments in the UK are being attacked an average of 84 times a week by hackers (McCue, 2002). According to the United Reporting and Alerting Scheme (UNIRAS) (McCue, 2002), government departments reported a total of 13,146 hacking attempts between the periods of 1999 to the year 2002. Most of these proved unsuccessful with access being denied in 12,929 cases, but sensitive data was stolen or disclosed on 10 occasions and in 23 cases files were deleted or damaged. In August 2000, UK's Civil Aviation Authority had issued a safety alert about a new threat to air passengers: hackers taking over air traffic control transmissions and giving pilot bogus orders (Daily News, 2000). The government recently proposed amendments to the CMA to update it with more expansive provisions and stiffer penalties. Some of the proposed amendments was to give the police and judiciary the greater 'legal clarity' when dealing with computer crime (Espiner, 2006). The proposed changes would alter the law regarding launching denial of service attacks, the creation of tools that could be used for hacking and bot attacks (Espiner, 2006). The amendments had been approved as part of the Police and Justice Act 2006. To further supplement the enactment, UK's new FBI-style crime fighting agency, ie, The Serious Organized Crime Agency (SOCA) had announced a range of new measures to tackle online crime gangs, such as a science laboratory to research emerging technologies that criminals might exploit (Thomas, 2006).

5.2. Singapore Computer Misuse Act 1993

The main legislation dealing with computer crimes in Singapore is the Computer Misuse Act 1993 (CMA), modeled after the United Kingdom's Computer Misuse Act 1990. In 1998, the CMA was further amended to address new attacks that had evolved with the spread of Internet (e.g. denial-of-service attacks). It also recognized that some computer systems were critical to Singapore (e.g. banking and finance systems, emergency services and public service systems) and thus the Act meted out harsher punishment for offenders who secured unauthorized access to such systems (Goh, 2005). In 2003, the CMA was amended again to make provisions in two specific areas. The first area was for the Minister of Home Affairs to be able to authorize a person or an organization to take steps necessary to prevent or to counter a threat to national security, before an offence has been committed. The provision also granted added protection for the informants of such threats. The second area was for certain offences under the CMA to be compounded, thus allowing the police greater flexibility in taking action in incidents of minor offences (Hamzah, 2005).

The number of cyber crime cases in the year 2001 was 137, and this figure rose to 151 in 2003 (Hamzah, 2005). The Singapore Government has given this issue a great attention due to its seriousness and high impact on Singapore economy. In a reported Singapore case of 2000, a 17 year old student pleaded guilty to three charges of hacking vis-à-vis unauthorized access to computer materials, unauthorized modification of the contents of a computer and unauthorized access to a computer service under the CMA (KPMG, 2005). The accused was sentenced to two months imprisonment on each of the three charges. In this case, the court viewed the seriousness of the offence and imposed a custodial sentence on the accused even when there was an absence of tangible damage caused to the victim companies. The absence of tangible damage was counterbalanced by the immeasurable inconvenience which the victims had to put to in establishing the extent of the accused's intrusion into their systems. They further averred that the offences here were crimes of conduct, liability for which was not dependent upon the occurrence of a prohibited result (KPMG, 2005).

In 2001, saw two lawyers convicted under S. 3(1) CMA when they were charged for unauthorized access to the database of their former employer whilst serving out their resignation notices (Hamzah, 2005). The two lawyers had on separate occasions copied confidential files from their employer's computer server using a zip drive.

5.3. U.S. Federal Computer Intrusion Laws

The US has the longest history among all countries discussed in terms of countering and controlling computer crimes (Grabasky, 2001). The US is a

Federal Republic and its Constitution allocates lawmaking authority between the federal and state levels in accordance with certain principles (Grabasky, 2001). Due to its political structure, computer related crime legislation and enforcement remain largely under state jurisdiction of prescription, adjudication and enforcement (Grabasky, 2001). The Department of Justice (DOJ) prosecutes hacking under Computer Fraud and Abuse Act (CFA) (Grabasky, 2001). The CFA punishes the knowing transmission of a program that causes damage to a 'protected computer' or the intentional access of a protected computer that results in damage.

Following the September 11, 2001 events, the CFA was amended to significantly expand the Justice Department's ability to prosecute those who commit computer crimes anywhere in the world (U.S. Dept of Justice, 2002). Nearly every major corporation in the U.S. has been victimized by computer crimes in the past 10 years – many of them repeatedly and by employees, according to the 2005 Computer Crime and Security Survey conducted jointly by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI) (CSI/FBI, 2005). Those reporting their organization experienced unauthorized use of computer system in the last 12 months increased slightly from 53 percent in year 2004 to 56 percent in the year 2005 (CSI/FBI, 2005).

6. ANALYSIS AND CONCLUSIONS

Based on the information presented above on computer crimes in the three continents, it seems that Malaysia is in a position to learn something from the experience of others. Another thing to note is the similarity between Malaysian CCA, Singapore's CMA and UK CMA. An interesting observation about the Singapore experience that Malaysia could benefit from is that given the increase in computer related crimes and computer abuse, the CCA has to ensure that they are able to embrace new circumstances without having to be amended and/or undertaking systematic reviews of their legislative requirements with respect to the prevention and control of computer related crimes. Malaysia could learn also from the many sub-laws that the U.S. has in treating the various types of computer crimes. Malaysia could follow U.K. in terms of setting up an agency to handle all cases related to cyber issues. By establishing such an agency, they would be able to procure skilled law enforcement personnel to deal with computer and even broader IT related crimes. At present, the prosecutions of these cases are handled by the Malaysian police, and as stated above, some of them lack the technical skill and know how to deal with the ever evolving changes and breaches that computer crimes bring about.

Despite the global agreement on the seriousness of the problem of computer hacking and other forms of computer crimes, there are still many issues and questions to be resolved. Despite the extra-territorial laws such as Malaysia's

CCA has, there is a problem in terms of international agreements between countries regarding this matter. Before Malaysia can implement this aspect, there must be a global agreement in order for Malaysia to get the cooperation of other countries. There will be many scenarios and problems in regard to this. One problem is the determination of where the offense occurred in order to decide which law to apply. The other issue is unless there are proper extradition treaties between Malaysia and other countries, a criminal action against a foreign hacker might be difficult to prosecute even though it has been detected. The existing extradition legislation will have to be reviewed to include computer crime as one of the extradition offence (Extradition Act 1992).

Another problem is obtaining evidence and ensuring that the offender can be located and tried before a court. Some computer experts have criticized the CCA in failing to clarify the lines between evidence and identity. As computer surfers are bound to copy or modify information on the Internet for their own benefit, this blurs the identity lines. The problem is how they can be tracked down when the data or content need not be physically removed for unauthorized access to be detected (The Star, 1997). Law enforcement and regulatory vacuums exist in some parts of the world, certainly in those settings where the state has effectively collapsed (Grabosky, 2001). Even where state power does exist in full force, the corruption of individual regimes can impede international cooperation.

We must also seriously question whether the criminal law is the best way to tackle hacking. This is not a new observation. The Council of Europe expressed the same sentiments (Council of Europe, 2003). However, in a decided case in Singapore in the year 1999, the Honourable Chief Justice of that case added that it should not be discounted for Singapore to introduce more severe punishments which encompasses amongst others, caning, life imprisonment or even perhaps the death penalty. His remark was made in line with that when national survival becomes increasingly more and more dependent on the full operation of such computer systems, any unauthorized access to such computers should warrant even more severe punishments (PP v Tan Fook Sum, 1999). Due to the fast growth of technology and the number of people involved in activities related to information technology, computer crimes are difficult to detect or prevent.

The success of Malaysia's CCA will rely on whether it can be enforced effectively, which depends on the effectiveness of the techniques for detection and investigation in face of this rapidly changing technology. Malaysia does not lack laws or regulations that promote the development of new technologies. Legislation in respect of intellectual property rights, is adequate, progressive and in compliance with the best international expectations. However, Malaysian authorities have a tendency to stop at the law- making stage and to

neglect administration and enforcement. Malaysia's track record in law enforcement of commercial crimes in the physical world has been far from satisfactory and it is unlikely that the enforcement machinery will be able to cope effectively with prosecuting the complex crimes in cyber space (Loong, 2001). It is unlikely that Malaysia will on its own have the means to police crimes committed on the internet. Greater international cooperation and a system of data collection and sharing is required (Loong, 2001).

It is not disputed that the enforcement agencies may have scant understanding of internet based laws or lack the technical knowledge which will be necessary for them to detect criminal behaviour. Very often the issues that may be relevant in the physical world do not have any relevance in cyberspace. Enforcement agencies must not only be good prosecutors they must also have a good working knowledge of cutting edge technologies (Loong, 2001). According to NISER (2003), computer forensic experts need to have relevant experience and specialized training which are now lacking in Malaysia. This in turn contributed to the lack of cases being prosecuted, and therefore leading to the increase of the number of computer crimes (NISER, 2003).

If Malaysia was serious about being a leader in the development of cyber laws there is a need to update the approaches to the CCA, which was based on the law which was created before the widespread use of the Internet. Otherwise, despite the availability of other modalities of constraints such as technology and management best practices, Malaysia would be stuck to the legal solution that was only appropriate in that era. Several strategies can be undertaken such as expanding the scope of the provisions to include a broader category of offenders, adopting a creative way of sentencing the offenders and creating a compliance model for information security.

In the provision of substantive offences, the CCA is wider in scope than the UK legislation. However, the CCA does not go as far as adopting the Singapore legislation on providing for unauthorized use or interception of computer services (SCMA, 2003) or providing for the concept of a "protected computer" (SCMA, 2003). Conforming to the UK approach, the penalty imposed would appear to be related to the type of offence and the severity of that offence, rather than to the degree of damage caused by unauthorized access or modification as evidenced in the Singapore statute. This suggests that not only the UK approach of sentencing, but also the justification for the criminalization of unauthorized access, are being adopted in Malaysia without modification, thus bringing whatever problems that have occurred or are occurring in the UK to Malaysia. Since the CCA is modeled based on the UK Act, and it was created before the Internet development, it may not be effective in dealing with new Internet-related activities such as denial of service.

Malaysia can learn much from the experience of the U.S. in this area. The many cases that are available from the U.S. Department of Justice (U.S. Dept.

of Justice, 2007) should act as a good reference for Malaysia to fine tune its current Act to include the many possible ways of hacking and intrusion. Malaysia can use these cases as a guideline to comply with their political, culture and economic environment, and to come up with a more comprehensive set of laws with proper implementation and enforcement.

7. REFERENCES

Annamalai, N. *"Cyber laws of Malaysia: The Multimedia Super Corridor"* (1997), 12(12) Journal of International Banking Law pp 473-481

Bellouin, S. (2001) Computer Security – *An End State*, Communications of the ACM, Vol. 44, No. 3, pp. 131-132

Carr, J., and Williams, K. (2000), Securing the e-commerce environment: enforcement measures and penalty in the computer misuse legislation of Britain, Malaysia and Singapore, *Computer Law and Security Report,* 16 (5) 295-310

Chik, Warren (2006), *Computer Crime, Cyber Crime and Challenges to Law Making: A Critical Comparative Study of the Adequacies of Computer Crime and Cyber Crime Legislation in the United States, the United Kingdom and Singapore*. Paper presented at the VI Computer Law World Conference, Edinburgh, Scotland, UK http://www.law.ed.ac.uk/ahrb/complaw (visited 5th January 2007)

Council of Europe, *The Convention on Cyber Crime (ETS No 185)*, available at http://conventionc.coe.int/treaty/EN/cadreprojects.htm

CSI/FBI Computer Crime and Security Survey, 2005

Durst et. al (1999) *Testing and Evaluating Computer Intrusion Detection Systems*, Communications of the ACM, Vol. 42, No. 7, pp. 53-61

"Different kind of hijacking is taking place in the skies" at http://abcnews.go.com/sections/us/DailyNews/FakeAirTrafic 000829.html (Visited on 22nd March 2002)

Edappagath, Ajmal (2004), Cyber-Laws and Enforcement by Ajmal Edappagath, Vol. 14, No. 3, December 2004, available at http://www.iimahd.ernet.in/egov/ifip/dec2006/dec2006.htm (Visited on 12th January 2007)

Eschelbeck, G (2000), *Active Security – A proactive approach for computer security system,* Journal of Network & Computer Application, V. 32 (2), pp. 109-130

Grabasky, P. (2001), *The Global and Regional Cyber Crime Problem*, The University of Hong Kong Center for Criminology

Granger, S. (1994), *"The Hacker Ethic"*, Ethics in the Computer Age, ACM Proceedings, pp. 7-9

"Hackers target UK national infrastructure" by Andy McCue, March 26, 2002 at http://www.vnunet.com/News/1130416 (Visited on 12th January 2007)

"Hacking as Political Weapon in Malaysia" USA Today Tech Report, June 12, 2000

Hamzah, Z. (2005), *E-Security Law and Strategy*: LexisNexis and Malayan Law Journal

Hassan, Wan Faizal Wan, *"Malaysia Internet Country Overview*". International Telecommunications Union Workshop on the Internet in South East Asia, Bankok, Thailand 21-23 November 2001

Hiong, Goh Swee (2005), *Computer Crime Law in Singapore*, pp 83-90 in Zaid Hamzah (eds), E-Security Law and Strategy

http://www.cdt.org/security. The Center for Democracy & Technology website for the recent changes in the U.S. Computer crime laws following the events of September 11th, 2001. (Visited on 22nd March 2002)

http://www..gilc.org/privacy/coe-letter-1000html. The Council of Europe noted the lack of legislation in the areas of authorizing phone tapping and computer crime, but went on to observe that "criminal law is not the central instrument in controlling or steering harmful behaviour" (Visited on 12th January 2007)

http://www.gosci.com/prelea990301.htm, March 5, 1999 (Visited on 12th January 2007)

http://www.hmso.gov.uk/acts1990/Ukpage19900018_en1.htm (Visited on 22nd March 2002)

http://www.kevinnitnick.com. The case of Kevin Mitrick was a highly publicized case. He was arrested in 1995 in Raleigh, N.C., after he was tracked down via computer by Tsotomu Shimomura at the San Diego Super Computer Center. (Visited on 22nd March 2001)

http://www.mdc.com.my/msc.comm/html/cyberights.01.html. The set of laws introduced in Malaysia in 1997, covering computer crimes, copyright, telemedicine and digital signature were referred by the Malaysian Government as "cyberlaws" (Visited on 12th January 2007)

Hull, G. (2000), *An Introduction to Issues in Computers, Ethics and Policy,* Vanderbilt University (not published)

KPMG (2005), *An overview of computer crimes in Malaysia*, Isssue 3/March 2005, pp 1-4

"Lord: We need better cyber crime laws" by Tom Espiner, 21st June, 2006 at http://management.silicon.com/government/0,39024677,39159761,00.htm (visited 10th January, 2007)

Loong Caesar (2001), *Malaysia's Legal Framework for Promoting Technology*. http://www.asiasociety.org/speeches/caesar.html (visited on 12th January 2007)

Multimedia Development Corporation, Malaysia, *Malaysia Cyberlaws. See* Malaysian Cyberbills at: http://www.nitc.my (visited at 12th January 2007)

Masden, W. (1998), CIA & NSA Sound Alarm Bells on INFOWAR, *Computer Fraud and Security*, V. 1998 (8), 1998, pp. 8-9

Malaysia Computer Crime Act 1997

Nair, D. *"Cyber law Makers Must Look Into Hackers Minds"*, FT Asia Intelligence Wire, April 25, 1997, p B41

National ICT Security and Emergency Response Centre (NISER): *Is Cyber Crime Reigning On No Man's Land*, NISER's Quarterly Bulletin, 2004, Vol. 1, pg. 4

National ICT Security and Emergency Response Centre (NISER): *Statistics on Cyber Crime May Not Be Real"*, NISER's Quarterly Bulletin, 2004, Vol. 1, pg. 4

Nurris Ishak (2005), *"In Malaysia, it's a hackers heaven"*. New Straits Times, 15th May, 2005

"New crackdown on cyber crime" by Daniel Thomas, 11th May, 2006 at www.itweek.co.uk/computing/news/2155797/cracfkdown-cyber-crime (visited 12th January, 2007)

PP v Tan Fook Sum (1999) 2 SLR 523, the Honourable CJ made certain remarks that it may not be discarded that punishments may be increased, if warranted

Posch, R. (2001) Will the Internet Ever Be Secure? Journal of Universal Computer Science, Vol. 7, No. 5, pp. 447-453

Preliminary Court Report Population and Housing Census 2006, published by the Department of Statistics, Malaysia, 2006

Report "Half of smaller and midsize companies will suffer Internet attack", CNN Technology News, October 12, 2000

S. 4(1)(a) Malaysian Computer Crimes Act (MCCA), S. 4(1)(b) MCCA

S. 4(1)(a) MCCA

Sani, Rozana, (2003), "*Push for more forensic experts"*. Computimes, 31st October, 2003

Singapore Computer Misuse Act 1993 (SCMA) (as amended in 2003)

U.K. Computer's Misuse Act 1990

U.S. Computer Fraud and Abuse Act was created in 1984

U.S. Department of Justice (USA) website: http://www.cybercrime.gov/cccases.html (Visited on 12th January 2007)

UNIRAS website: http://www.uniras.gov.uk (Visited on 22nd March 2002)

Yang, T. Andrew (2001) Computer security and impact on computer science education, Proceedings of the sixth annual CCSC northeastern conference on The Journal of Computing in small colleges, Middlebury, Vermont, pp. 233-246

ZDNetAsia (2001), *Malaysian Parliament hackers took it as a challenge*. 2nd January, 2001

CO-AUTHOR'S NOTE

Ms Janaletchumi Appudurai, an outstanding lecturer from the Department of Business Studies at HELP University College died in a water rafting accident on 21st January 2007. At HELP University College, she was involved in the teaching of Business Law, Company Law and Law of Employment for both the Charles Stuart University and University of East London Bachelor degree programme in Business.

She was a person of rare quality. The contribution she made to our department and our university and the imprint she has left goes far beyond what is known by each one of us who had the privilege to work with her or to count her amongst our friends.

She was a dedicated and committed staff, well liked by colleagues and students. She was always full of energy and initiatives and she will go all out to make business law an interesting subject to business students.

The combination of her vision with the capacity to provide a practical approach towards the teaching of business law made her a leader in many spheres.

She was also very enthusiastic towards doing research and presenting papers at Conferences and Seminars. She has written and published numerous articles related to HRM.

The incident that happened on 21st January 2007 was a tragedy.

As a colleague and friend, she was always compassionate and supportive. Her death is not only a personal loss to me but also a big loss in the academia at HUC.

Chitra Latha Ramalingam