Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Malaysian Law and Computer Crime

This paper attempts to describe the Malaysian Computer Crimes Act 1997 (CCA 1997) and provide important guidelines for a successful computer crime investigation. The enactment of the CCA 1997 is a step in the right direction for a developing country such as Malaysia as she attempts to push herself towards a Knowledge-based economy. However, having laws alone will not be sufficient to carry out trials against cyber criminals. We will be looking into other important elements in a computer crime case, which includes good ...

Copyright SANS Institute
Author Retains Full Rights

AD

Malaysian Law and Computer Crime
By Chong Yew, Wong (GSEC Practical Assignment v1.2f)

1. Introduction

This paper attempts to describe the Malaysian Computer Crimes Act 1997 (CCA 1997) and provide important guidelines for a successful computer crime investigation. The enactment of the CCA 1997 is a step in the right direction for a developing country such as Malaysia as she attempts to push herself towards a Knowledge-based economy. However, having laws alone will not be sufficient to carry out trials against cyber criminals. We will be looking into other important elements in a computer crime case, which includes good criminal investigation and the need to maintain close cooperation between different organizations and countries. In addition, this paper will also briefly look at notable computer crime cases, especially those in the United States. By understanding the nature of these cases, we would be able to greatly appreciate some of the more "common" threats that are often neglected or taken for granted.

2. Overview of the Computer Crimes Act 1997 (CCA 1997)

We will start by taking a closer look at the CCA 1997, which is one of the many cyber laws enacted in Malaysia. The following is a summary of the offences relating to misuse of computers as extracted from the "Explanatory Statement" of the CCA1997:

a) Seeks to make it an offence for any person to cause any computer to perform any function with intent to secure unauthorised access to any computer material.
b) Seeks to make it a further offence if any person who commits an offence referred to in item (a) with intent to commit fraud, dishonesty or to cause injury as defined in the Penal Code.
c) Seeks to make it an offence for any person to cause unauthorised modifications of the contents of any computer.
d) Seeks to provide for the offence and punishment for wrongful communication of a number, code, password or other means of access to a computer.
e) Seeks to provide for offences and punishment for abetments and attempts in the commission of offences referred to in items (a), (b), (c) and (d) above.
f) Seeks to create a statutory presumption that any person having custody or control of any program, data or other information when he is not authorised to have it will be deemed to have obtained unauthorized access unless it is proven otherwise.

(http://ktkm.netmyne.com.my/contentorg.asp?Content_ID=158&Cat_ID=1&CatType_ID=17&SubCat_ID=40&SubSubCat_ID=95)

The CCA 1997 essentially covers crimes resulting in violation against any of the "three (3) bedrock principles" of security (confidentiality, integrity and availability). Specific mention of how CCA 1997 covers the "availability" principle is in order, as it is not spelled out clearly in the Act. The "availability" principle is covered under item (c) above as the definition of

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

modification includes modification of any contents of any computer that takes place if any event occurs which impairs the normal operation of a computer.

One note worthy section from the Act is that it provides much authority to the police officer investigating the case.

> "Whenever it appears to any police officer of or above the rank of Inspector that there is reasonable cause to believe that in any premises there is concealed or deposited any evidence of the commission of an offence under this Act, and the police officer has reasonable grounds for believing that by reason of the delay in obtaining a search warrant the object of the search is likely to be frustrated, he may exercise in and in respect of the premises all the powers mentioned in subsection (1) in as full and ample a measure as if he were empowered to do so by warrant issued under that subsection."

This empowers the officer of an Inspector rank and above to conduct warrantless searches. The downside to this provision is that the case may be challenged on the basis that evidence was obtained unlawfully. Any rash acts by the police officer may jeopardize the entire case.

In addition to that, the Act also allows that any police officer arrest without a warrant any person whom he reasonably believes to have committed or to be committing an offence against this Act. Further to this, the Act also allows police officer's above the rank of Inspector to conduct search at premises without warrant should the officer believe that delays may effect them obtain necessary evidence. Both these provisions greatly empower the police officer and allow them to put the law in their own hands. Imagine this scenario, a 20-year old student had been arrested by mistake because the police officer "had reasonable reasons to believe" that the student made an attempt to have unauthorized access to a computerized system. The incident can be both embarrassing for the authority and traumatic for the student in question. In terms of computer crime, most investigation and arrest would occur after the first attack/attempt of attack, and thus it would be sensible for the police or relevant authority to conduct search or arrest upon gaining the proper warrants and evidence.

Part 3 of the CCA 1997 states that anyone, regardless of nationality and location when committing an offence, will be dealt with as if the offence were committed in Malaysia. Offenders found guilty may be sentenced to a jail term or a monetary fine or both. The length of the sentence or fine will depend on the offences that the offender is found guilty of. The challenge is therefore to get the offender to Malaysian shores for a trial to be made against him/her. From some of my research work for this paper, it was interesting to note that in some cases offenders were "tricked" into entering a particular country through fake job offers or interview opportunities.

3. Ingredients for an effective computer crime trial

Now that we have covered the CCA 1997, we will focus our attention to the key ingredients that are important to form an effective case in a computer crime investigation.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The first of course is the enactment of appropriate laws, with the aim of protecting the computer crime victims, to serve as a deterrent to would be hackers (the penalty should be severe enough) and to provide a legal means of prosecuting those who are found guilty of committing such crimes. In Malaysia, the punishment may range from 3 years to 10 years imprisonment and/or a monetary fine of between RM 25,000 to RM 150,000. Note that stiffer penalties will be given if it is found that the guilty party had intention to cause injury when committing the crime.
- Next of course is to have a group of specially trained prosecutors in the area of computer crime. The challenge for this group of prosecutors is that they have to be generalist on the subject of computer security and information technology. This is to enable them to tackle the various technologies that they may come across when dealing with cyber criminals.
- The success of a computer crime investigation is also highly dependent on the effectiveness of the investigative team. More and more computer crime divisions are being setup within the police force around the world. In United Kingdom (UK) for example there is the Metropolitan Police Service Computer Crime Unit. This unit deals with crimes that relates to the Computer Misuse Act in the UK. There is even a new establishment called the National High Tech Crime Squad (UK) to deal with technology related crimes that run across conventional police boundaries and require specialist investigation skills. The key point that is highlighted here is trained specialists are required to carry out investigations in computer crime cases.
- The global nature of criminal activities requires that strong ties be forged between enforcement agencies around the world.
  - United States Attorney General Janet Reno gave a good example of how complicated a crime investigation could be when technology involved in the case resides in another part of the world. "An officer may quickly find himself or herself in the middle of a case with international implications. For example, during the raid of a drug dealer's home, an officer might download data from the suspect's network account only to find out later that the data was stored in a foreign country and the download violated that country's law."
  - Bruce Schneier in his book "Secret and Lies" also brings up the point that "the global nature of the Internet complicates criminal investigation and prosecution". Bruce raises the question of which state or country's law should be used for prosecution, will it be from where the data/attack originated from or where the data/target is located or even where the data/transmission passes through? Personally, it really depends on two things. The first consideration is the effectiveness of the laws in a particular country and the second consideration would be how easy would it be to bring the suspect to trial in the preferred country.
  - The Malaysian Parliament website that was hacked on December 2000 was traced to IP addresses in Brazil and France. The relevant authorities in those countries were contacted for assistance in the investigation. This clearly shows the importance of strong working relationships between authorities in countries around the world.
- Early communication with Internet or Network Service Providers
  - In his article "Tracking a Computer Hacker", Daniel A. Morris highlights this as one of the important elements when tracing a hacker. ISPs may have in their possession key records that will help track a hacker. However, in most cases, proper documentation (e.g. a court order) will be required from the investigators before an ISP will corporate.
- Security training and awareness – do's and don'ts when attacked

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Another ingredient that is required for a successful investigation is the actions (pre or post action) of the system administrators of an attacked system. This includes the activation and storage of adequate audit and system logs. This is important as it is equivalent to looking at footprints or fingerprints in the physical world.

- Use of traditional investigative techniques
  - Finally, investigators in computer crime cases should also utilize traditional investigative techniques in their work. This point was clearly pointed out by Daniel A. Morris as he pointed out that it would be necessary to identify the actual person using a particular computer or user ID to commit a crime. Take for example a trace that leads to a computer in a college lab. As hundreds of students make use of the lab, day in day out, the investigator would have to fall back on more traditional techniques such as physical surveillance or getting information from students or lab assistants.

4. Computer Crime Case & Lessons Learned

For this section, we will be focusing on computer crimes in the United States, as it is the most up-to-date and publicly available information on computer crimes over the Internet. From these cases, we will be able to better comprehend and appreciate the "Internet Threats" that are out there.

a. U.S. v. Ventimiglia (M.D. FL). This case is about an ex-employee intentionally damaging his company's computers. How does he get in to the computer facility you may ask? Well, pretty simple if you are still buddy with an existing employee. This clearly shows that you may have the best door access system or security cameras in the world, but when there is collusion with internal or "trusted" employees, you can hardly do much to stop the crimes from taking place. However, what can be done is probably to allow strict disciplinary action against employees violating policies such as allowing unauthorized persons to restricted areas. This will at the very least result in an individual thinking twice before committing any rash acts.

b. U.S. v. Morch (N.D. CA). This is another example of an internal threat. Basically, an employee on his last day of duty copies out proprietary information and was caught. This brings up a couple of precautionary measures that may be considered when dealing with staff resignation.
   i. Consider removing or limiting access to staff that has tendered their resignation; or
   ii. Monitor the action of the staff from the period he/she tenders their resignation letter.
   iii. Where possible, change password to the administrator or other IDs that is known by the staff leaving.

c. U.S. v. Oquendo (S.D. NY). In this particular case, a computer security expert was found guilty of computer hacking and electronic eavesdropping. This case once again shows that Internet threat can come from within an organization. In this particular case, the employee does the damage while still with the company and began exploiting his earlier efforts remotely.
   i. The challenge to system administrators is to basically know what is supposed to be on their systems. This knowledge along with regular review of the software or

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

applications on the system will ensure that any new or unknown software or rogue files are detected and scrutinized.

d. U.S. v. Smith (D. NJ). Unlike the previous 3 cases highlighted above, which were internal threats, this case dealt with threats coming from and infecting through the Internet. David L. Smith pleaded guilty for creating the "Melissa" virus and causing millions of dollar worth of damage. One thing to learn from this case is that fighting computer criminals, especially those which leverages on the Internet as a medium of attack, requires collaboration between multiple parties. In this particular scenario, America Online and ICSA.net were amongst the key contributors to the successful investigation of the case. Although this was more of an availability attack, Smith could be faced with a 5-year federal prison sentence.

e. U.S. v. Gregory (N.D. TX). This case is classified as a telecommunication fraud and computer hacking. The case was chosen for discussion, as it is different from the four cases above. Among other things, it includes use of stolen access devices, PIN obtained from other hacking organization and stolen credit card information. With access to these equipment and information, Gregory could make free teleconferences at the expense of the Telecommunication Service Provider. An important lesson or reminder that we can take from this case is that the hacker network is large and they are willing to trade information amongst themselves. To me there are both pros and cons about this situation. The obvious disadvantage against the authorities is that they are fighting against a very large network of cyber criminals. The advantage for the authorities is that there are more leads to follow up on. The more people who are involved or know about a crime, the higher the likelihood of obtaining useful leads to the criminals.

5. Last Words

Before I conclude the paper, I recently came across a piece of news that state a group of hacker cracked into a Sudanese bank and obtained information about the Al-Qaeda terrorist organization and its leader Osama bin Laden. They have apparently handed over the information to the Federal Bureau of Investigation or FBI. However, the authorities have neither denied nor confirm the incident. The question here is that if these announcements were indeed true, how should this case be treated? Would the authorities be indirectly "approving" hacking activities if they were to use the information for the interest of national security? Would it be better if the hackers would have gotten the information and passed it on to the authorities without publicizing it? In a virtual world where laws are still maturing, it is difficult to draw a clear line as to what is right or wrong, especially when justice needs to be served. Other hacker organizations may use this as an opportunity to begin hacking into sites, which are linked to terrorists but for their own agenda. Lawmakers and authorities definitely have a great task ahead of them for defining internationally acceptable cyber laws.

6. Conclusion

Computer crime definitely must be taken seriously. Attacks can come from a computer across the room or computers located in another country. The threat could be external or it could be internal. It may have financial impact, it may deal with child pornography or it may be related to cyber terrorism. Because of the number of computer crime cases that

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

has increased over the years (and many more unreported), the development of computer crime laws and policing initiatives must grow in tandem. Tackling computer crime is similar to tackling computer security; you have to start from the basics and address one thing at a time. As long as there is a system in place to punish the wrongdoers, as long as there is public awareness of the potential seriousness of such crimes, I believe that there will be much headway in computer crime law and investigation in the coming years in Malaysia and around the world. One important element that I found to be similar between most of the cases was the strength of the investigation team and the support it has received from its counterparts whether locally or internationally. With that I would like to sum up the paper with a quote from Barry W. Mawn, the Assistant Director in Charge of the New York Office of the Federal Bureau of Investigation, "This investigation and these charges should dispel the notion that using a computer to commit criminal acts literally a world away from one's victim provides a zone of safety from law enforcement scrutiny. In fact, the growth of computer related crime in recent years has resulted in a closer coordination among law enforcement agencies around the world. This investigation demonstrates the cooperation of both American business entities and our international law enforcement partners to address 21st century crime" (http://www.cybercrime.gov/bloomberg.htm).

Bibliography

1. Attorney General Janet Reno Addresses the High Technology Crime Investigation Association 1999 International Training Conference, September 20, 1999.
http://www.usdoj.gov/criminal/cybercrime/agsandie.htm

2. Department of Justice's (US) Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice.
http://www.usdoj.gov/criminal/cybercrime/index.html

3. Department of Justice – Computer Intrusion Cases. Last updated October 1, 2001.
http://www.cybercrime.gov/cccases.html

- "Ex-GTE Employee Pleads Guilty to Intentionally Damaging Protected GTE Computers", March 20, 2001. Last updated March 22, 2001. (http://www.cybercrime.gov/VentimigliaPlea.htm).
- Press release from the US Department of Justice, March 21, 2001. Last updated 3 May 2001. (http://www.cybercrime.gov/MorchPlea.htm).
- "Computer Security Expert Sentenced to 27 months Imprisonment for Computer Hacking and Electronic Eavesdropping, June 13, 2001. Last updated on 14 June 2001. (http://www.cybercrime.gov/OquendoSent.htm).
- "Creator of Melissa Computer Virus Pleads Guilty to State and Federal Charges, December 9, 1999. Last updated, December 14, 1999. (http://www.cybercrime.gov/melissa.htm)
- "Computer Hacker Sentenced", September 6, 2000. Last updated September 25 2000. (http://www.cybercrime.gov/gregorysen.htm)

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- "Three Kazak Men Arrested In London For Hacking Into Bloomberg L.P.'s Computer System", August 14, 2000. Last updated, August 31, 2000. (http://www.cybercrime.gov/bloomberg.htm).

4. Malaysian Computer Crimes Act 1997
http://ktkm.netmyne.com.my/contentorg.asp?Content_ID=80&Cat_ID=1&CatType_ID=17&SubCat_ID=40&SubSubCat_ID=15

(If you are having trouble accessing the above link, please go to the general site of the Malaysia Energy, Communications and Multimedia Ministry's Homepage at http://www.ktkm.netmyne.com.my - Go to menu item => Organisation => Jurisdiction => Ministry of Energy, Comm and Multimedia => Computer Crimes Act 1997)

5. Morris, Daniel A. "Tracking a Computer Hacker". Last updated July 10, 2001. http://www.usdoj.gov/criminal/cybercrime/usamay2001_2.htm

6. Puvaneswary, S. "Police Seek Help From The Two Countries To Track Down Those Responsible". 17 January 2001. http://www.niser.org.my/news/2001_01_17.html

7. Schneier, Bruce. Secret and Lies. John Wiley & Sons, 2000.

8. Stafford, Ned. "Sudan Bank Hacked, Bin Ladden Info Found – Hacker", Newsbytes. 27 September 2001. http://www.newsbytes.com/news/01/170588.html.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**