Impacts and Effects on implementing e-laws in Thailand

Amnuay Sala, Chonawat Srisa-an

Faculty of Information Technology, Rangsit University

Abstract

Economic and social development is becoming increasingly dependent on digital technology. However, the benefits of digital technology were also increasingly prone to criminal exploitation so that it threatened the development of e-business. Computer crimes have had a negative impact on businesses, particularly those that rely heavily on electronic transactions. However, these cyber-crimes would weaken consumers' confidence in doing business online

Cyber crime is a term which is used to describe the act in which computers and networks are target for criminal activity. In Thailand, The issue of cyber crime has been continuing to grow dramatically as a controversy for several reasons. We need laws that protect us from computer crimes. Therefore, There are six related law has been lunched including Electronic Transactions Law, Electronic Signature Law, Electronic Funds Transfer Law, Data Protection Law, National Information Infrastructure Law, Computer Related Crime. Electronic Transactions Law is the first law that lunched in April 2002. On 18 July 2007, the Computer Crime Act B.E.2550 (2007) came into force. However, the effect and impact of those laws is widely causes many controversy and business problems. In this research, we try to survey and summarize what is the cause of crime and the effect of implementing e-law in Thailand.

Index Terms— e-law, Electronic Transactions Law, cyber crime law

1. Introduction

The Oxford Reference Online defines cyber crime as crime committed over the Internet. The Encyclopedia Britannica defines cyber crime as any crime that is committed by means of special knowledge or expert use of computer technology. (www.crime-research.org/library/Cybercrimimal.html) Examples of widely committed cyber crimes are social engineering frauds, hacking, identity theft, child pornography, online gambling, securities fraud, and cyber-stalking. The rate of these crimes continues to increase as the number of computer literate people in our society increases. Most computer crimes are no different from other crimes, and computer criminals should be held responsible for the damage they cause.

One of the main types of computer crime is identity theft. Identity theft is a crime involving illegal usage of another individual's identity. Types of identity theft include financial identity theft, criminal identity theft, identity cloning, and business/commercial identity theft.

Another example of identity theft: a criminal legally obtains personal identifiers, and then clones someone to them for concealment from authorities. This may be done by a person who wants to avoid arrest for crimes, by a person who is working illegally in a foreign country, or by a person who is hiding from creditors or other individuals. Unlike credit-dependent financial crimes, these crimes are non-self-revealing, continuing for an indeterminate amount of time without being detected.

Another classic example of identity crime occurs when a criminal obtains a loan from a financial institution by impersonating someone else. The criminal pretends to be the victim by presenting an accurate name, address, birth date, or other information that the lender requires as a means of establishing identity. Even if this information is checked against the data at a national credit-rating service, the lender will encounter no concerns, as all of the victim's information matches the records. The lender of the loan has no simple way to discover that the person is faking his identity, especially if an original, government-issued identification can't be verified. This type of crime is considered non-self-revealing, although authorities may be able to track down the criminal if the funds for the loan were mailed directly to him. The criminal keeps the money from the loan, the financial institution is never repaid, and the victim is wrongly blamed for defaulting on a loan he never authorized.

(Wiki) Another main type of cyber crime is called "hacking". In computing, the term hacking is used in a wider sense to mean using software for enjoyment or self-education, not necessarily involving unauthorized access. However, once people begin to hack for malicious purposes, that is when is becomes a crime. The most destructive for of hacking is the creation of a virus. A computer virus is a computer program that can copy itself and infect a computer without permission or knowledge of the user. Another type of computer infection is called a worm. A worm travels from computer to computer while a virus travels from file to file. Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the

hard disk. Others are not designed to do any damage, but simply replicate themselves and perhaps make their presence known by presenting text, video, or audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behavior and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

2. Methodology

In this research, we conducted a survey to find out how people feel about the issue of cyber crime. Firstly we provide the respondents with some brief information, they seemed to be able to answer the questions.

The first question asked: "Do you think cyber crime is not serious to yourself or your business?" More than fifty percent of the respondents said yes. A few people said that it depends on the type of cyber crime. Some people said that computer crimes such as identity theft and child pornography should definitely be treated as legitimate crimes, and that the people who commit them should be treated as criminals.

	Yes	No
1) Do you think cyber crime is not serious to yourself or your business?	58%	42%
2) Does your computer have virus protection software?	29%	71%
3) Do you open up emails sent to you by unfamiliar email addresses?	35%	65%

Table 1. Questions and results from survey

The second question I asked was: Does your computer currently have virus protection software installed? I was not surprised when all of the respondents answered yes. Pretty much all new computers are sold with virus protection software which can be activated simply. However, this doesn't necessarily mean that people are using them properly and updating them on a regular basis. I advised the respondents to try to update there virus protection software as much as possible so there computer can eradicate even the most recent viruses.

The third and final question I asked was: Do you open up emails sent to you by unfamiliar email addresses? A shocking number of people responded with yes. Once the respondents answered yes to that question, I suggested that they research the dangers of opening phony emails.

A recent Microsoft survey[5] of the cybercrime laws in Asia Pacific includes a regional study of the internet security, spam, and privacy and security laws. The 13 countries included in the survey are Australia, China, Hong Kong, India, Indonesia, Japan, Malaysia, New Zealand, The Philippines, Singapore, South Korea, Taiwan and Thailand. In 2007 Bangladesh, Sri Lankra and Pakistan has also enacted cybercrime bills. This study indicates the degree of implementation of cybercrime laws in the 13 counties (Table 2).

Moderate-Strong Implementation	Moderate-Weak Implementation	Very Weak Implementation
Australia	China	India
Hong Kong	Japan	Indonesia
New Zealand	Malaysia	The Philippines
Singapore	South Korea	Thailand
Taiwan		

Table-2 Implementation of Cyber crime Laws in Asia Pacific Region.

From Table-2, The long-awaited Computer Crime Act, which comes into effect on August 23, 2008. The new law was also designed to enhance electronic commerce and national security, and should as a result encourage online transactions by creating a safer cyber-environment that is more conducive to business for all.

3. Movement in Thailand

At the National Electronic and Computer Technology Center (NECTEC) in 2002, The development of computer emergency response teams (THAI-CERT') has been found and played a vital role in responding to computer crime as well as combating the spread of malicious code. Since 2002 , the ICTs Ministry has replaced the National Electronic and Computer Technology Center (NECTEC) in overseeing Internet content. Quite recently , the ICTs Ministry has created a new regulatory body called the " Cyber inspector " of which the board comprises a group of selected senior government officials and high-ranking corporate executives. The task of the Cyber-unspector, which is sub-divided into five working groups , is mainly to oversee questionable materials , computer crimes and hacker problems as well as to make

out that Sanook is ranked first among Thai portal websites since 2005 and its traffic is ranked 321 among 500 most popular sites in the world

decisions on blocking of websites. The Ministry operates a hotline , which is (theoretically) accessible through the Internet and telephones. At present , the ICTs Ministry has about 1,300 websites on its blacklist (already blocked) out of about 10,000 websites that have been notified.

Alongside , the Office of National Police , which has been an active force in regulating Internet content from the outset , is cooperating closely with the ICTs Ministry and ISPs in filtering out illegal and harmful content as well as in tracking violators on the Net to prosecution. The Office of National Police also has a hotline that receives notification about problematic content from the public. Noticeably, the approach undertaken by the ICTs Ministry and the Office of National Police depart significantly from that of NECTEC in the past. While NECTEC focuses more on promoting awareness about Internet risks through its research and public education activities , the ICTs Ministry-Office of National Police alliance are more keen on passing and enforcing regulatory measures and blocking of questionable content.

The Computer Crime Act, the first cyber crime law 2008, will have a positive impact on both avid "netizens" and non-computer users alike by protecting online privacy and ensuring Internet security. The Computer Crime Act is Thailand's first serious attempt at dealing with crimes in cyberspace. The goal of the act is to plug the loopholes in existing laws in order to empower law-enforcement agencies to more effectively deal with crimes committed via the computer or Internet. Such crimes include hacking, unlawfully accessing computers or network resources, and the unauthorized interception of e-mails or data transmission with the aim to commit theft or do harm to others. Without this law, law-enforcement officials would be unable to apply the Criminal Code and criminal procedures in order to go after cyber-criminals.

4. Controversy and obstacle

4.1) The Royal Thai Police force meanwhile will be developing its capacity to investigation computer crimes. Since there are currently too few officers who specialist and are well versed in computer crime investigation and evidence-gathering techniques, police will refer cases of computer crime to the ICT Ministry for investigation.

4.2) The law will require service providers such as ISP to back up information, such as IP addresses and user logs, which would increase their cost of doing business. The companies bear a higher maintaining cost and staffs. This rule will benefit on the Storage Vendor. All ISP or service providers will need to keep a giant log for 90 days.

4.3. People will have to think twice about such innocuous activities as forwarding e-mails containing information or pictures of other people in compromising positions, or circulating URLs of websites that offer content such as pornography. Senders will now have to consider the impact of this material on others because those forwarding such material can also be prosecuted for infringing on others' rights to privacy. From our survey, a lot of teenagers do not agree on this rule. They think that some innocent teenagers don't know this rule and might do this unintentionally.

4.4. Even though Thailand is through with its first cyber law, Computer Crime Act, the service providers have been unable to provide satisfactory standard security solutions because many procedures come into action within limited staffs. In order to comply this law, most providers need to invest more on infrastructure and personals.

5. Conclusion

THAI's Cyber crime could reasonably include a wide variety of criminal offences and activities. The scope of this definition becomes wider with a frequent companion or substitute term "computer-related crime." Criminals have adapted the advancements of computer technology to further their own illegal activities and these inventiveness have however, far out-paced the ability of law enforcement agencies to react effectively.

There will be endless types of computer related crimes in the future. Computers have enabled people to commit an endless amount of crimes. It also can be much harder to catch a criminal when he is committing a crime behind a computer screen.

In response to the rising crime rate, authorities have continued to intensify their efforts against computer crime. The rate of these crimes is expected to continue to increase as the number of computer literate people in our society increases. Authorities need to continue to crack down on cyber crimes because they apply the same damage as real crimes. They also threaten an extremely large number of people. Anyone with internet access is a potential target for these crimes. As virus protection software advances, and knowledge on other types of computer related crimes increases, hopefully we will find a way to eliminate the threat of internet crime.

Therefore, within the law enforcement agencies, a set of rules must be developed to address the various categories of computer crime. As such, investigators will know what and which materials to search and seize, the electronic evidence (logs and information traffic) to recover, and the chain of custody to maintain. However, the higher maintaining cost and personals will lead to the new problem domain from Thai Business.

References

1. By Gene J. Koprowski. Cyber Crime News Retrieved 11/18/07 http://www.pcsndreams.com/Pages/Articles/IDTheft.htm
2. (Wiki) Wikipedia Contributors. Identity theft, Retrieved 11/18/07 http://en.wikipedia.org/wiki/Identity_theft
3. Brian Winter. Computer Crime Statistics, Retrieved 11/18/07 Http://www.cybercrime.gov
4. Bangkok Post Editor. "A Chilling Idea for Internet Law". www.bangkokpost.com/law_alert/ISOC_alert01.html
5. Grant Julie Inman (2007), First Technical Assitance Seminar on International Implementation of APEC Privacy Framework, Key Note Speech, Julie Inman Grant, Microsoft Corp, Australia.
6. Borland, John, and Pelline, Jeff. "Hack Leads Point to California Universities". news.cnet.com/2100-1023-236827.html
7. Reuters. "2d Briton Is Charged In Computer Spying". query.nytimes.com/gst/fullpage.html?res=9C03E2D61539F937A15755C0A960958260
8. Walton, Val. "Two Sentenced for High-tech ATM Thefts".www.al.com/news/birminghamnews/index.ssf?/base/news/1206089188208770.xml&coll=2 - 26k
9. Wikipedia. "Computer Crime". en.wikipedia.org/wiki/Computer crime
10 Wikipedia. "Computer Fraud and Abuse Act". en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act
11 Wikipedia. "Zombie Computer". en.wikipedia.org/wiki/Zombie_computer
12 Wilson, Clay. "Botnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress". Updated January 29, 2008. fas.org/sgp/crs/terror/RL32114.pdf