

eCrimes on the Internet - A Global Challenge

Kuldeep Nagi

Fulbright Fellow-2006
Lecturer-ICT
College of Internet Distance Learning (CIDE)
Assumption University
Bangkok, Thailand 10452
<http://www.elearning.au.edu>

Abstract

The Internet has permeated almost all areas of our social lives. Millions of people around the world are using the Internet for work, education, business and pleasure. In the last 10 years we have also seen increasing crimes on the Internet such as porno, sex tourism, buying and selling of pirated goods, identity thefts, intellectual property thefts, credit card and bank frauds, hacking and cyber-terrorism. After the disastrous events of 9/11 in USA a whole new industry has cropped up to protect the ordinary citizens from these crimes. As the Internet based services gain popularity and people begin to trust online agencies to provide more and more services, an important question is raised: how the Internet technologies will safeguard the interest of the increasing number of consumers on the Internet, especially in Asia where the law enforcement is not adequate. Who are the stakeholders in the growing eBusinesses and Cybercrimes? What are the business and legal implications of increasing cybercrimes and does the Internet pose a global crisis? While there are laws available to deal with the cybercrimes, they are difficult to enforce, especially in Asian Pacific countries. This paper examines the

increasing role of the new Internet technologies in promoting the biggest boundary-less eBusinesses, such as eBay, a host of ePorno, eSex and eDating services, Google, U-Tube, Hotmail, Yahoo and Victoria's Secret and will also analyze the global challenges posed by increasing cybercrimes.

1. Introduction: Cybercrimes and the Media

A survey of 725 cities conducted this year in USA by the National League of Cities for the anniversary of the 9/11 attack shows that cyber terrorism ranks with biological and chemical weapons atop officials' lists of fears. Concern over Cyber terrorism is particularly acute in Washington D.C., USA. As is often the case with any new threats the events of 9/11 have changed the way we think about the cyber world and cybercrimes. Take a look-

- ◇ Private companies all over the world have hastily deployed security consultants
- ◇ World-wide an entire new industry has arisen to grapple with cybercrimes and its ramifications
- ◇ Think-Tanks have launched new projects and every week they issue

new white papers, sometimes with white lies

- ◇ Experts have testified to its dangers before US- Congress and other international organizations.
- ◇ And of course, whole host of new software and hardware solutions.

are being sold to protect public and private targets. And as usual the popular media have trumpeted the threat with such front-page headlines as this one in The Washington Post last June: “Cyber- Attacks by Al Qaeda Feared, Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say.” It’s no surprise, then that the cybercrimes now ranks alongside other serious crimes in the public consciousness.

Unfortunately media in Thailand and other Asian countries have also heightened into this fear. Bangkok Post (July 22/07) headlines like “Information and Communications Technology (ICT) Ministry” website hacked or another sexy headlines like “Website hackers traced to Europe” with some sketchy details like these are common these days. “Pranksters who hacked into the Information and Communications Technology (ICT) Ministry website posting a picture of Thaksin Shinawatra along with anti-dictatorship statements on its homepage, may be European-based Thais with sympathies for the ousted government, officials said. ICT Minister Sitthichai Pookaiyaudom said an investigation into the IP addresses of the hackers showed the web attacks were carried out from Europe. Officials said attacks were launched from three countries, one of them Germany [1]”

There’s one place where the rise in computer crimes is paying off: Hollywood. In the 21st century, computer crime—from hacked passwords to identity theft—is the stuff of celluloid dreams Hollywood has

gone beyond the headlines and been playing this game for decades, but the first—and still most influential – computer crime movie came in 1983 with “War Games.” Matthew Broderick played a teen geek (and future icon and role model for generations of hackers) who nearly starts World War III after launching a thermonuclear war game between the U.S. and Russia. This year in the movie “Firewall,” Harrison Ford made security engineers into heroes when he portrayed Jack, a banking maniac whose firewall system becomes a sticking point for a gang of ruthless crooks. Ford is ordered to transfer \$100 million into a crook’s account—or his family members will die. Of course, Harrison Ford manages to save the bank—and the day—but a larger question looms: can computer crimes be sexy? In another block buster movie “Live Free or Die Hard” released in May 2007 when someone hacked into the computers at the FBI’s Cyber Crime Division, the Director decides to round up all the hackers who could have done this. The Director instructs the local police department to take care of it. And one of the cops John McLane is given the task of bringing a hacker named Farrell to the FBI. When a criminal plot is in place to take down the entire computer and technological structure that supports the economy of the United States (and the world), it’s up to a decidedly “old school” hero, police detective John McLane, to take down the conspiracy, aided by a young hacker Farrell.

Ironically, the rise of interest in Hollywood cyber-drama hasn’t created a boom in consumer awareness. The reality of cybercrimes is more intriguing than these popular films could imagine. Consider the real-life of good Michael and Ruth Haephtrati who seemed like any dot-com entrepreneurs. The young married couple, living in London, operated an Internet security firm called Target Eye. But when the two were taken into custody last May, it turned out they were

targeting more than anyone suspected. The Haephratis are accused of being the masterminds behind one of the biggest cases ever of commercial espionage; they allegedly pawned services to help some of Israel’s biggest companies infiltrate each other’s inner workings. Their weapon of choice: spyware [2]. For years, spyware—insidious software that secretly installs itself on a computer and then logs and disseminates a user’s activity—and its dirty cousin, adware, which unleashes unwanted pop-ups, have been a growing nuisance online. The National Cyber Security Alliance has reported that 80 percent of home surfers have had spyware or adware on their computers. Infection is so widespread that there are now Web sites devoted to chronicling spyware horror stories.

2. Financial Damages:

In the good old days before the internet, cybercrimes were mostly trespasses into the public and private networks and defacements of web sites. Now, cyber criminals are primarily motivated by financial gain. As such, the old image of the kid living on Pepsi or Coke and junk food, while doing sixty four hour hacks, has been replaced by a darker and much more complex persona, one who is well organized and strictly focused on making money off of anybody they can victimize.

But just how much damage can cybercrimes cause to a country’s economy? In 2005 it cost \$67 billion to U.S. companies, according to an estimate based on the Federal Bureau of Investigation’s 2005 Computer Crime Survey, released in January 2006. The FBI questioned 2000 public and private organizations in four states in USA and extrapolated some of the results to the rest of the country. It found that viruses and spyware were the most common problems reported while the effects of viruses and

worms were the most costly [Table-1]. The attacks came from 36 different countries, with half of all the attacks originating in the

Table-1 Financial Losses

Financial losses from security attacks reported by respondents to the FBI	\$32 million
Respondents’ losses from viruses and worms	\$12 million

United States or China. A small fraction of the organizations reported the incidents to law enforcement officials. Most of the others were either unaware that the attacks were illegal or believed that law enforcement would not help them—and might even harm them [3]. 90% of organizations sampled by the FBI suffered a cyber security attack, 84% of respondents had virus problems and only 9% of the organizations reported the problem to authorities. 79% of respondents that had spyware attacks. Whether it is an experiment by an amateur virus writer somewhere in Hong Kong, done just for the individual’s personal entertainment, or a carefully planned and executed for-profit scheme of an Israeli spyware company, a computer security attack is annoying and damaging. Between July 1 and December 31, 2006 United States was top country for malicious activity accounting for 31% of world wide total (Table-2).

Table-2A. Malicious Activity by Countries (Source – Symantec Corporation, 2006)

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank
1	United States	31%	1	1
2	China	10%	3	2
3	Germany	7%	7	3
4	France	4%	9	4
5	United Kingdom	4%	4	13
6	South Korea	4%	12	9
7	Canada	3%	5	23
8	Spain	3%	13	5
9	Taiwan	3%	8	11
10	Italy	3%	2	8

Table-2B. Malicious Activity by Countries (Source – Symantec Corporation, 2006)

Overall Rank	Country	Command And Control Server Rank	Phishing host Rank	Bot Rank	Attack Rank
1	United States	1	1	2	1
2	China	4	8	1	2
3	Germany	3	2	4	3
4	France	14	4	3	4
5	United Kingdom	9	3	6	6
6	South Korea	2	9	11	9
7	Canada	5	7	10	5
8	Spain	15	16	5	7
9	Taiwan	6	6	7	11
10	Italy	10	14	12	10

For each of the malicious activities taken into account for this measurement the United States ranked number one by a large margin with the exception of bot-infected computers. It ranked second for that criterion, 12 percentage point lower than China.

3. There is no such thing as Perfect Security:

3.1 Risk Management by Organizations

What can organizations do about the pervasive cyber security threats? The companies need to stop measuring security investments just in monetary terms and start thinking of security as a kind of marathon. It's a like lifestyle and it should affect every decision you make every day. Information security entails people, technology and processes. Appropriate measures have to be in place and operating properly at all times in each of these areas in order for information to be secure. And in this modern age, any enterprise that does not have a complete information protection scheme in place is just begging to become a victim. There are many recognized areas that are part of information assurance and since some of these are dependent on each other there is also an implied sequence to how they are implemented and maintained.

Logically, the first step in any properly targeted response is to identify what has to be protected and then categorize what threatens it. Once the actual threat picture is known a concrete and repeatable process can be installed. The elements that are involved in establishing such a process are the same as they would be for any other type of organized effort- effective policies, sustainable procedures and good operational practices. After, and only after, a concrete security infrastructure is established, are the security countermeasures developed and deployed. These countermeasures represent the organization's approach to securing all of the tangible and intangible areas of threat. The countermeasure set comprises the specific personnel, physical, software based, business continuity and legal and regulatory compliance controls that address the known risks, as well as the specific form of the

network, encryption and application and operating system software security procedures and technology. Done correctly the information assurance solution will satisfy two criteria. First, it will protect all information of value, in whatever form. That includes written as well as electronic assets. Second, the safeguards to ensure reliable protection will be in-place and operating properly at all times. That ensures that the security will be sustainable. Both of these criteria have to be satisfied for an organization to be truly protected and that costs money but given the consequences and likelihood of the alternative, it is worth the price [4].

3.2 Risk Management by the Internet Users

It's one thing to fall for a phishing scam, which can be avoided easily enough by simply calling a financial institution before submitting private financial information online, but other forms of electronic identity theft are not as easy to protect against. Known as pharming, this insidious spin-off of phishing can be exacted via viruses, such as the notorious Banker Trojan, or hacker exploits of firewall servers. "This could rapidly worsen as attack systems become more automated," says Peter Cassidy, secretary general of the Anti-Phishing Work Group, an association of business and law enforcement organizations in USA. Sometimes, however, identity theft doesn't rely on the consumer's role at all. Such was the case last year when MasterCard International revealed that names, accounts, and security codes of 40 million customers had been compromised by a hacker attack; of these, 68 000 customers were deemed to be at particularly high risk. The phishers feed a larger epidemic of identity theft that is reaching epic proportions. The FTC found that, every year, almost 10 million people are victims of identity theft, costing consumers

US \$5 billion and businesses \$48 billion.

Last spring, the teachers, students, and workers at the University of Kentucky Federal Credit Union received an email that seemed routine enough: Because of a problem in the electronic banking system, customers needed to verify their account information. After clicking a link, they were taken to a page with the bank's logo where they were instructed to enter their personal identification numbers. Unknown to the 20 victims, however, their financial details were not going back to the campus, they were zipping to South Korea, where they would be used to create pirate debit cards. The only hint of a scam was tucked away in the site's Web address, which read "http" instead of the usual "https," designating a secure site. The naive users had just been phished. And they're not alone. Phishing, social and technical engineering aimed at hustling surfers' personal data, is an insidious form of identity theft that's on the rise. According to a report by IBM, phishing attacks hit an all-time high, rising by 226 percent in 2005. The Federal Trade Commission (FTC) receives nearly 200 000 reports of phishing attacks every year.

This is fairly common these days. Exercise good online hygiene by downloading browser security patches and by running both firewalls and anti-virus software. Make sure everything is up to date. And don't get lulled into thinking that cybercrime only happens in the movies

3.3 Internet Laws in Asia-Pacific Region- Lack of Enforcement

The government is stepping up its fight against spyware. Recently the U.S. House of Representatives passed two anti-spyware bills, which could send spyware peddlers to prison for up to five years or face \$3 million in fines. But the ultimate protection is to

download and update anti-spyware software such as Ad-Aware or Spybot Search and Destroy. Experts suggest shelling out the extra cash for programs that automatically monitor spyware invasions. In 202 United States and 29 other nations signed a treaty establishing common tools and rules for fighting Internet crime. On Nov. 23, 2002 foreign ministers from the United States, Canada, Japan and South Africa joined their counterparts in 26 other countries in signing the Council of Europe’s “Convention on Cybercrimes” an international treaty designed to harmonize laws and penalties for crimes committed via the Internet. Since that time little has been accomplished in terms of implementing the treaty.

A recent Microsoft survey of the cybercrime laws in Asia Pacific includes a regional study of 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 Lanka and Pakistan have also enacted cybercrime bills- none of which have been seriously implemented.[5] This study indicates the degree of implementation of cybercrime laws in the 13 countries (Table-3)

Table-3 Implementation of Cybercrime Laws in Asia Pacific Region

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		

In countries with strong to moderate implementation common weakness involves the implementation around misuse of device offences. In countries with moderate to weak implementation when the criminal offenses occur the current domestic legislation is applied very narrowly. In India the Information Technology Act of 2005 takes a Civil Liberty approach. The new IT Amendment Act) Amendment Bill of 2006) contains some offences correspond to some of the computer related and ancillary offences. Thailand Computer Offences Act was passed by the Thai National Legislative Assembly in May 2007 by a vote of 11 to 1. It aims to disabling of computer systems and establishes a number of criminal offences. The critics of the law say that the recent action to block YouTube and other sites, the COA passed by Thai government gives more censorship powers than fight cybercrimes.

Summary

As the usage of the Internet grows the cybercrimes will also become more prevalent as well as more sophisticated. Although there is a growing awareness of the need to enact stronger cybercrime laws, to achieve the commitment from the global community, especially the Asian Pacific countries remains a big challenge. Asian Pacific countries will have to understand the benefits of strong implementation of the cybercrime law. Targeted bilateral and multilateral outreach to Governments and closely aligned cybercrime laws should become a top priority of all nations. Cybercrimes are a global challenge that requires a concerted global response.

References

- [1] Bangkok Post (July 22/07) available online at URL
http://archives.mybangkokpost.com/bkk/archives/frontstore/news.html?click_page=16&textcat=General%20News&cmd=keepbook_text
- [2] Laurianne McLaughlin, Rosemary Clandos, (2003), "News," *IEEE Security and Privacy*, vol. 01, no. 4, pp. 8-11, July-August,
- [3] Symantec Internet Security Threat Report Volume XII: September, 2007
- [4] Yee Fen Lim (2003), "Law and Regulation in cyberspace," *cw*, p. 34, *Second International Conference on Cyberworlds (CW'03)*.
- [5] Grant Julie Inman (2007), First Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, Key Note Speech, Julie Inman Grant, Microsoft Corp. Australia,