

UNESCAP REGIONAL EXPERTS CONFERENCE

7-9 JULY 2004 Bangkok Thailand

E-commerce Legal and Regulatory Systems in Asia and the Pacific: Current Challenges and Capacity Building Needs

Current challenges of developing a legal infrastructure for securing e-commerce

by
Assoc Prof Harry SK Tan

Abstract

The new electronic communications technologies that allow us to find useful information and to communicate quickly and easily has evolved into a necessary part of our everyday lives. Unfortunately, the same technologies are fundamentally insecure and have become a target as well as a means for cybercrime and criminal activity. The capabilities of the new age criminals are growing and it is only a matter of time that their ranks will swell beyond the means of law and its enforcement agencies. Governments and law agencies are now finally bring their resources and attention to bear on this real economic and social problem. This paper highlights the growing security issues and the crimes faced by law agencies, businesses and governments. For any national programme to develop E-Commerce, in addition to a technologically secure infrastructure, a cohesive and supporting legal infrastructure is necessary. This paper will review the necessary elements for the proactive development of the law, security policy and education programme for securing E-Commerce.

About the Author

Harry SK Tan is the Director of the Centre for Asia Pacific Technology Law & Policy and a Senior Fellow at the Intellectual Property Academy. He is an Associate Professor of Law at the Nanyang Business School, Nanyang Technological University. He is the principal lecturer of the "E-Business: Law Policy & Strategy", "Law of Information & Technology" and "Legal and Ethical Issues of Information Technology" courses at the Nanyang Business School. Prof Tan has been involved in the field of technology law for nearly 10 years had been involved in advisory roles in the management of legal risks in electronic commerce and information technology. He was also a member of the team of consultant that drafted the new technology laws for the Dubai Internet City and Dubai Port Authority. His current research interest is in the development of the law and regulation of Electronic Commerce and its impact on businesses. Prof Harry Tan is also a Fulbright Scholar and Visiting Scholar at the Berkeley Centre for Law & Technology at University of California.

NOTICE: The information provided in this article is not intended to be nor is it a substitute for formal legal advice, but is only intended as a general guide and discussion of the issues involved and is non-exhaustive. Readers should consult qualified legal professionals for advice in relation to their e-commerce issues.

Current challenges of developing a legal infrastructure for securing e-commerce

by

Harry S K Tan*

1. Background - The Cybercrime threat to E-Commerce

In a relatively short time since the introduction of user friendly web technologies, the Internet has succeeded in positively altering the way we live, study, teach, communicate, spend our money and carry on business. There is a growing reliance on these online products and services by users and as a result, businesses are going online in response to the market demand. However, even as businesses identified the new opportunities, criminals have also similarly recognised the potential for crime through the new electronic medium. This growth in the incidence cybercrimes and security incidents fundamentally undermines the trust needed for commerce to grow on the Internet.¹ As captioned in Peter Steiner's famous cartoon in *The New Yorker* in July 1993, "*On the Internet, nobody knows you are a dog*", he succeeded in coining the core cause of a multitude of problems that e-commerce face today. The new communications technologies allow almost anyone especially the criminals to deceitfully pass oneself off as someone else trustworthy and reliable for the purpose of personal gain.

Conversely, without specific technologies like public key infrastructure and digital signatures, proving one's identity to strangers online is a near fruitless exercise. While such security technologies are able to resolve identity issues, it has proven to be both difficult and expensive to implement them successfully.²

Another dimension of problem in securing E-Commerce is the openness of the technology that continues to be evolving. Reports continue to be made of new and ingenious ways in which

* **ALL RIGHTS RESERVED.** Associate Professor of Law at Nanyang Business School, Nanyang Technological University. He is also the Director of the Centre for Asia Pacific Technology Law & Policy (CAPTEL) <http://captel.ntu.edu.sg>. Please email comments to: prof@e-business-law.com. Please note that this draft version is a working paper.

¹ The Carnegie Mellon CERT Coordination Centre reports that in 2002 there were 82,094 security incidents which increased to 137,529 cases in 2003 – a 67% increase.

² John Leyden, "PKI: the Key to e-success?" *VUNET.com*, 9 August 2000. It is estimated that a pilot PKI implementation will cost between US\$80,000 to \$120,000.

cyber criminals or hackers gain access to servers and computer networks with ease through poorly configured and un-patched operating software and applications.

The growth of business online with the increasing sophistication of technology coupled with the general low level of user understanding and knowledge of electronic security, provides an ideal environment for the commission of cybercrimes.

Criminals in general commit crimes for all kinds of reasons or motives. Their continued involvement in criminal activity is probably due to their belief that they will be able to get away without being suspected, apprehended or even identified. While criminals may have their reasons for being deluded as to their abilities for crimes in real-space, many have found that crimes committed in cyber-space or the virtual world are much harder to prevent or detect. Cybercrimes allows the perpetrator to be in a location some distance away from the act itself which gives rise to the difficulty of conclusively identifying and apprehending the criminal.

Fortunately, businesses have since realised that it is a necessity to keep in step with new technologies being developed for the prevention of online crime. This includes providing consumers with basic safeguards such as passwords, system firewalls, Secure Sockets Layer (SSL) sessions and payment systems that provides a generally high level of security but at a low cost to the consumer. Unfortunately, while many of these new technologies are efficient in what they were designed for, i.e. directly securing the information and transactions exchanged, they are not able to guarantee the unwary merchant or customer from being defrauded by the more astute cybercriminals. As a result of such security concerns and the increasing number of reports of cybercrime and fraud, consumers generally hesitate from disclosing personal and credit card data on the Internet.

When the cybercriminals directly hack into systems and networks that have not been secured, businesses face loss of proprietary data, intellectual property, and online access to customers and suppliers due to breaches and service interruptions.

In order for the Internet to contribute to economic growth and human development, it must be trustworthy and secure. Lack of trust and security jeopardizes development goals that could be supported by a widely accessible and widely trusted Internet.

1.1 Factors for the growth of cybercrime

The growth of cybercrime can be attributed generally to the following:

Technology

Easy availability of new technologies with high operational speeds, capacity and connectivity makes unlawful activities easier to escape detection. Conversely, the majority of cybercrime victims are not technologically sophisticated or equipped enough to prevent, detect or deal with computer crime;

Low Levels of Awareness

The lack of awareness of how to maintain a minimum level of security with regard to personal information or electronic property presents opportunity and targets for the cybercriminals;

Fear of adverse publicity

In some cases when a crime is detected, businesses have been reluctant to report criminal activity because of their concern about the adverse publicity, which can cause embarrassment, loss of public confidence, investor loss, or economic repercussions.

Outdated Law & Regulation

The criminal laws of some jurisdictions have not caught up with the challenge of new technologies. While some countries may have addressed the threat, some of these laws are already in need of amendment to address the new kinds of cybercrimes. Further, only a handful of countries have attempted to address the issue of prosecuting cybercrimes committed by criminals from another jurisdiction.

Law Enforcement Agencies

Many law enforcement agencies lack the technical expertise as well as sufficient regulatory powers and equipment to investigate and prosecute cybercrimes.

1.2 Types of Cybercrimes

Cybercrime or computer related crime is a collective description covering a myriad of online offences.³ Here is a sample list of crimes that have been commonly committed:

³ See <http://www.ftc.gov>.

1. Web site defacement or vandalism
2. Denial of service attacks on websites and online services
3. Theft of customer data
4. Theft of electronic intellectual property
5. Theft of Internet & Telephone services
6. Sabotage of data or networks
7. Financial and On-line Securities Fraud
8. Forgery, illegal interception & ID Theft
9. Payment card fraud & e-funds transfer fraud
10. Pornography/Child Pornography; cyber-stalking
11. On-line Gaming/Betting
12. Commercial/Corporate Espionage
13. Extortion & criminal conspiracy communications
14. Disruption of essential or critical network services

Not all of these cybercrimes however require the illegal access to computers. One such example is online fraud. This is a more elegant crime in that it usually does not require the criminal to attack the security systems but to work around it. Similarly, a deception perpetrated through the use of a computer or electronic communications in the course of an online transaction would be an online fraud. Online fraud can be committed within Internet relay chat rooms, via electronic mail, message boards or on Web sites.

1.3 Who are the Cybercriminals?

The cybercriminals who are capable of illegally gaining access to computers and servers to commit these crimes are commonly called hackers and crackers. These are the skilled individuals who are capable of the more technical cybercrimes. This however is longer the norm. While most are still working independently, there are growing concerns about organised crime using the new technologies to commit cybercrimes.⁴ Cybercriminals can be categorised into three groups which reflects their motivation:

⁴ "Organized Crime and Cybercrime: Synergies, Trends, and Responses" - Global Issues August 2001 US Dept of State's Electronic Journals <http://usinfo.state.gov/journals/itgc/0801/ijgc/gj07.htm>

Cybercriminals wanting recognition

- (a) Hobby hackers
- (b) IT professionals
- (c) Politically motivated hackers
- (d) Terrorist organizations

Cybercriminals not wanting recognition

- (a) Financially motivated hackers (corporate espionage)
- (b) State sponsored hacking (National Espionage, sabotage)
- (c) Organized Criminals

Insider Cybercriminals

- (a) Disgruntled or former employees seeking revenge
- (b) Competing companies using employees to gain economic advantage through damage and/or theft

2. Requirements for an effective legal infrastructure for secure E-Commerce

A regime or programme to create an effective infrastructure for securing E-Commerce requires a concerted and comprehensive development of several elements including laws, policies, industry self regulation, technical standards and law enforcement.⁵ Together these elements can provide a positive environment and infrastructure to support the growth of E-Commerce.

2.1. Empowering and equipping law enforcement

Law enforcement agencies all over the world are meeting the threat of electronic crime by developing highly trained and well equipped law enforcement officers to handle the increasing sophistication and international reach of cybercrime and fraud on the Internet. Officers on such teams would be trained on the latest technologies and computer forensics know-how. Specifically they are given appropriate training in the investigation, collection of electronic

⁵ An excellent effort was made in this respect was the *UNESCAP Draft Action Plan on Cybercrime and Information Security for the Asia Pacific Region*. The Draft Action Plan was adopted at the Asia-Pacific Conference on Cybercrime and Information Security, held from 11 to 13 November 2002, in Seoul, Republic of Korea under the auspices of United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), the Ministry of Information and Communication (MIC) of the Republic of Korea and the Korea Information Security Agency (KISA).
<http://www.unescap.org/icstd/documents/actionplans/cybercrime%20action%20plan.doc>

evidence and prosecution of electronic crimes. The training will be on a regular basis to counter the rapidly evolving nature of computer technologies.

Due to the technical complexities coupled with the grave legal issues raised by such crimes, each jurisdiction is developing the necessary teams of experts who are able to dedicate themselves to the investigation and prosecution of cybercrime.⁶ As the online customer will patronise any virtual shop at all hours of the day since the Internet operates around the clock, enforcement agencies should have their investigation experts available on a 24 hour and 7 day week basis.

Besides domestic training that is given, agencies are also given international exposure by participating in internationally hosted conferences or training sessions on the latest innovations and technologies or criminal investigation techniques. Co-ordinated training sessions between nations would go a long way in sharing information and ensuring that new methods are being shared quickly with neighbouring countries.

2.2. Public education, training and cybercrime reporting

Consumer education is more effective than any law enforcement action in preventing cybercrime or fraud being committed through the Internet. Consumers need to be empowered through education so that they enjoy a rewarding experience when transacting on the Internet. The effort to provide consumers with the necessary education should be increased through the combined efforts of government, business, and consumer groups. There should be organised programs for teachers and parents to supervise and guide their children in the responsible use of the Internet as a tool for studies and entertainment. There are various technological and non-technological tools that can be used to protect children from the risks of cybercrime: blocking and filtering software and following safety tips when using the Internet. There are several websites that give parents tips and guidelines to promote safer Internet experiences for their children.⁷

The Internet itself can be used to disseminate information to the public on fraud, privacy and technology-related issues. This is important as such information also reaches those fraudulent persons and businesses, thus acting as deterrence. Also, the Internet as a forum for such

⁶ An example of this would be The Federal Trade Commission (FTC) which formed an Internet Rapid Response Team; or the Singapore Criminal Investigation Department's *Technology Crimes Branch*.

⁷ www.getwise.org , www.americalinksup.org , www.cyberangels.org , www.parenttech.org , www.safekids.com , www.fbi.gov

messages is a low-cost and effective way to reach large and more or less unlimited consumer base.

There should also be a continuing education programme for public and private sector workers using computers on the current best practices as well as how to comply with the organisation's information security policies. The education programme should also include how each person is to report known cybercrimes – whether to employers or when personal computers are affected, directly to the correct law enforcement agency.

2.3. International Best Practices and Standards to Secure Computers and Networks

Law unfortunately, will not make networks and computers more secure. Even while strong and effective laws can be enacted and enforced, it is still fundamental that the physical security and the management of security must be in place to prevent security breaches. While businesses may demand software houses, solution providers and manufacturers to provide more secure products, security is inevitably a continual process within each organisation. Even governments have to consider their internal network security management as a process that requires constant care and attention.

Countries have begun to review and investigate what needs to be done to address the problem from both the public and private sectors.⁸ One such development is the governments of the Organization for Economic Co-operation and Development (OECD) that drew up the “Guidelines for the Security of Information Systems and Networks”.⁹ These guidelines are designed to develop a “culture of security” among government, business and users in an environment of worldwide expansion of communications network, increasing interconnectivity across national borders, converging technologies and ever more powerful personal computers.

An important and widely accepted standard for information security are the ISO17799 “Information technology - Code of practice for information security management”.¹⁰ Such

⁸ “eEurope 2005: Action Plan” http://europa.eu.int/information_society/eeurope/2005/index_en.htm. In this report, the private sector should develop good practices and standards and promote their consistent application in the context of “culture of security”.

⁹ See <http://www.oecd.org/dataoecd/16/22/15582260.pdf>

¹⁰ Visit the homepage of ISO or International Organisation for Standardisation - <http://www.iso.ch/iso/en/ISOOnline.frontpage>

internationally recognised standards are useful in that there is a certification process to maintain the high standards needed to keep the networks safe from harm. In addition, they provide assurance to clients and customers that the organisation has established best information security practices.

2.4. Effective Cybercrime Legislation

Every nation, as part of the efforts to promote E-Commerce trust and confidence, should have basic criminal laws against activities that attack the confidentiality, integrity or availability of computer data, computer systems and electronic networks. In order to fight cyber crime, there is a need to clarify what constitutes an offence or a crime especially in the global scenario the prosecution of transnational illegal activities are expected. Governments should agree on the definitions of certain crimes committed in the Internet environment. Laws must be enacted to criminalize hacking, illegal interception, interference of availability of computers and networks and unlawful access to systems.

An attempt to address the international nature of cybercrime and to develop a common standard for cybercrime law was made by the Council of Europe(COE) in the *Convention on Cybercrime* that was released in final form in June, 2001.¹¹ The Commonwealth also published a *Model Law on Computer and Computer Related Crimes* that was published in October 2002. The model law was developed by an expert group while reviewing in detail the provisions of the Convention on Cybercrime.

The main aim of the COE Convention is to pursue a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation.

The Convention includes a list of crimes and requires the criminalizing of such activities as hacking (including the production, sale, or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also

¹¹ The convention can be found at - <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>. Although thirty-four countries participated in the ceremonial act of signing the Convention in November, 2001, only six have actually ratified the Convention namely Albania, Croatia, Estonia, Hungary, Lithuania, and Romania.

requires each signatory state to implement certain procedural mechanisms within their laws.¹² There are provisions of surveillance powers for governments as well as the duty to help each other gather evidence and enforce laws..

Finally, the Convention requires signatory states to provide international cooperation to the "widest extent possible" for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their requests for assistance in the pursuit of criminals across national borders, something that is common in Internet crime.¹³

2.5. International cooperation of law enforcement agencies

For the growth of online commerce to continue, genuine businesses and consumers alike must feel confident that the Internet is safe from cybercrime. The Internet gives the criminal the ability to appear suddenly, commit the crime quickly then disappear without revealing their true identity or location. Often these criminals are located in a foreign jurisdiction. Thus, stopping them requires law enforcement officers to move just as quickly and often requiring co-operation from a spectrum of organisations representing government, businesses and consumer groups in the various countries. To be able to apprehend the international cybercriminals, greater co-operation and communication among international law enforcement agencies is required. Any collaboration among international agencies will also include the establishment of databases, joint law enforcement, and joint projects.

Unfortunately, many countries do not have the laws or the necessary skilled law enforcement personnel to deal with computer-related crime. This undercuts the efforts to battle a growing threat. With the proliferation of cybercrime in its myriad forms, what would be the best strategy to protect businesses and consumers? Certainly co-ordination between countries in the enforcement of unlawful conduct on the Internet is laudable. In practice however, this is likely to be rather difficult to achieve. The geographical and national borders, from the user's

¹² For example, law enforcement authorities must be granted the power to compel an Internet Service Provider to monitor a person's activities online in real time.

¹³ It is noteworthy however that the Convention has had its detractors. See http://crime-research.org/library/CoE_Cybercrime.html a paper that focuses on the convention's wide scope of powers accorded to the law enforcement agencies under the convention.

perspective, are almost non-existent. With the new technologies, Cybercriminals do not have to be in the country of the victim of the fraud to commit it.

As the victim and the criminal might be located in two different jurisdictions, governments need to review the traditional methods used to investigate conventional fraud offences. There should be in place a formal mechanism for seeking assistance and prosecution by the enforcement agencies of different jurisdictions rather than leaving it to the vague practice of professional courtesy. Furthermore, if there is no formal arrangement for mutual legal assistance in such investigations, such cases might be ranked as a lower priority since the victims live outside the jurisdiction. Accordingly, it would be ideal for a central cybercrime body to be set up to co-ordinate the efforts of all the agencies and eliminate the duplication of efforts.

3. Conclusions

It is inevitable that if criminals are willing to invest in technologies and adapt them to commit crimes in new unfamiliar ways and the law will take some time to catch up. While it is impossible to wholly eradicate cybercrime, it is possible to dramatically reduce it. This can be done through vigilant public education, industry leadership in standards development and compliance and using effective security technologies as well as having law enforcement agents equal in technical skill with the cyber criminals. However, most critical in the scheme of cybercrime management is the establishment of a balanced common standard for countries to co-operate on cybercrime law and prosecution.

=====