Chapter 7: Recommendation and Conclusion

7.1 The Way Forward

There is a sharp rise in phishing statistics as it evident from the values in various countries. May it be the number of hosting of phishing sites, or mails received about phishing, monetary loss either of the customers or of organizations. The main reason for losses/ success of frauds is ignorance on part of customer as well as service providers (bankers, ISPs, retailers etc). Prof N.P Singh, Professor of Management Development Institute, Gurgaon, from India stated that it requires stringent methods of educating customers and regular review of security related information of individual customers.[195] For example:

i. Customer should not be allowed to be the customer of financial institutions unless they read security related concern properly and provide a proof to the institutions that they are aware of security concerns. This could be done by pushing terms and conditions of being customer in pieces and unless customer runs though all pieces of information his/her application should not be accepted for being a customer. It will certainly act as an stumbling block to have more customer but new innovative methods can be devised so that customer did feel heat of these measures.

ii. There are many cases reported in the past with reference to inadequate characters of password in terms of sequencing and number. The institutions may devise a policy of secure password in terms of sequencing the characters or characters it self. In addition, policy must take care of size of the security related data. In addition, institution may analyze the pass word

[195] N.P Singh, "*Online Frauds in Banks with Phishing*", Journal of Internet Banking and Commerce, Aug 2007, Vol 12, No. 2

data base on regular interval for inadequacy and it may be communicated to the customers on real time basis[196].

iii. The information on incidents of phishing or similar serious crime should be made available to the citizens as early as possible and also out come of judicial process. In addition, new regulations must be made available through electronic means to all the citizens/ customers[197].

iv. Many organizations (Software developers or implementers) have developed anti-phishing solutions. The usage of these security tools may be encouraged through regulations. In addition, small organizations should be supported by states in making their electronic transactions secure[198].

vii. There is a need for better, easy to use and cost effective methods of authentication of customer transactions.

viii. To fight phishing, institutions must adopt a multi-pronged approach with minimum four components. (a) usage and development of new technologies to counter frauds, (b) educating customers with riders every where, (c) helping law reinforcement agency by way of providing information of the incidents, and (d) proper and regular stringent audit of online systems[199].

Phishing attacks in the world of online banking have become increasingly serious and spread more rapidly because simply access via the globally connected networks, how easy it is to not get perceived by computer users, and the dilemma that attackers gain monetarily without being caught. The sophistication of such attacks will likely increase over time and become less likely to be discerned from a legitimate email, web address, or web site, even

[196] Ibid
[197] Ibid
[198] Ibid
[199] Ibid

for experienced computer users. Online system vulnerabilities only aggravate this situation, making it difficult for users to battle against such attacks.

New technologies and standards are becoming more important than ever to deter and detect phishing attacks but we have to be realistic in how long it will take. No single technology can keep phishing at bay but there are ways to make phishing harder to accomplish and less appealing for the would-be phishers. Legislation is necessary for the prosecution of a crime after the fact. However, prevention is the better way to fight the problem

Importantly, companies should have disaster recovery plan in place to cover phishing attacks. Bank Negara Malaysia (BNM) Guideline stressed on consumer education will increase the awareness of the phishing threat and online vulnerabilities. Educating information technology users including individuals, corporate entities and organizations is a largely preventative measure. For example, consumer assistance through the media to better informs and alert consumers. It involves more than just educating them on security and other defensive or self-help measures. Likewise, they can provide valuable assistance in reporting, evidence gathering, investigations and enforcement. The existence of counter-scam technology and laws must not be allowed to engender a false sense of security and consumers should be informed and encouraged to report scams to a clearly designated government agency for further investigations and other actions.

Security insiders should applaud the growing public-private partnership and the increased attention to phishing issues so that information can be shared within the network of allies to expand incident-response capabilities to deal with the spike in phishing attacks. There is also a need for Malaysian government leadership to commit to fighting the online menace by giving more investigators, more funding, and more attention from lawmakers and upper

management, because as far as the legislation is concerned, the Malaysia legal position is still having loopholes to hook the phishers. The best model of law can be referred to is the California Anti-Phishing Act and the UK Fraud Act, which Malaysia should have their own legislation dealing with phishing, identity theft, account hijacking or any related matters.

In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized.

There must be a multifaceted and multipronged approach using a combination of both legally coercive and non-legal measures. The international legal framework should consist of a dual carriageway approach to the problem with specific treaties for each subject area that is susceptible to universally consistent treatment and model laws in areas that do not, so as to promote as similar and consistent a set of laws as possible for each category of crime. In that way, the overall effect is optimized.

The Cybercrime Convention and other regional and multilateral initiatives are useful insofar as they serve as strong policy statements and to some extent as undertakings, by governments to tackle what is clearly recognized as a collective problem that requires a collective solution. They also acknowledge and address the requirement for effective prescription, adjudication and enforcement in order for the solution to be truly effective. They serve as a necessary stepping-stone to a more effective and comprehensive treatment and they are often negotiated and discussed in fora that encourage understanding and consensus.

However, more needs to be done in order to effectively deal with the growing problem of computer-related crime. From the above analysis, there are some features that are integral to growing the international order in the cyber realm. Using cyber fraud and identity theft

as the case study and in the context of phishing, pharming and related forms of deception, the following requirements are deciphered[200]:

1. Prescriptive jurisdiction – This requires consistent worldwide criminalization of offences through applicable laws that have mutually enforcing effect, whether through extra-territorially applicable laws or a comprehensive network of same or similar laws or both.
2. Adjudicatory jurisdiction – Criminal procedure laws must ensure that offenders cannot avoid being brought to the courts in at least one country; provisions in a treaty requiring either enforcement or extradition can have that effect.[201] This eliminates or at the very least should drastically reduce the possibility of safe havens.
3. Enforcement jurisdiction – Even if a criminal is tried and convicted, effective enforcement of decisions is essential in order for the full effect of the system to work, particularly if the offender or his accomplices, instruments of crime or assets are in other jurisdictions. Consistent and reinforcing mutual legal recognition and enforcement treaties and provisions are required.
4. Administrative cooperation – Mutual legal assistance and cooperation in investigations, collection of evidence and other police matters are important. A strong international system of cooperation such as through Interpol as well as regional networks and a robust national infrastructure are important in this respect in order to successfully

[200] Warren B. Chik, "Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore"

[201] In some Terrorism Conventions, for example, there is a provision that requires parties that have custody of offenders to either extradite the offender or submit the case for prosecution. Other provisions of note are provisions that require "severe penalties" or that require parties to assist each other in connection with criminal proceedings brought under the Convention. See the list of Conventions Against Terrorism at the UN Office on Drugs and Crimes web site at: http://www.unodc.org/unodc/terrorism_conventions.html. See in particular article 7 of the Hague Convention for the Suppression of Unlawful Seizure of Aircraft of 1970 and the Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation of 1971 ("The Contracting State in the territory of which the alleged offender is found shall, if it does not extradite him, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case to its competent authorities for the purpose of prosecution…"). See also, Chapter II, Section 3 on jurisdiction and Chapter III, Section 1, Title 2 of the Cybercrime Convention on the principles relating to extradition. It is submitted that cyberspace is no different from its physical analogue (i.e. the world) when it comes to commonality of certain subject matters (e.g. terrorism and cyber-terrorism) and due to the commonality in nature and effect of human communication and intercourse (i.e. transnational interaction and extraterritorial effects).

identify, capture, try and convict cyber criminals. A network of domestic central specialized authorities connected to one another through one centralized international agency will be ideal.[202]

5. Pre-emptive measures – As far as possible, substantive law should have the effect of deterring and preventing offences from occurring rather than merely punish for offences that have occurred. This can be done through providing legal sanctions for preparation to commit offences that prescribes offences irrespective of its successful commission.[203]
6. Applicable laws (substantive) – Substantive laws must be rendered applicable to electronic transactions and digital assets including money and products; preferably through specific stand-alone legislation or new provisions, but otherwise through amendment of existing laws and definitions.
7. Applicable laws (procedural) – Procedural laws should be enacted or amended to facilitate the gathering of evidence and investigation of computer related crimes (i.e. computer forensics), and investigators and detectives must be equipped and skilled with the necessary expertise and technological know-how to investigate and deal with such offences and offenders.
8. Appropriate remedies – The law should create a credible and effective deterrent effect and sufficient punishment to suit the nature and severity of the offence.[204] Also where relevant, provisions allowing for rehabilitation could be useful, particularly if previous offenders, with their expertise, knowledge and connections, can be inducted into the

[202] Consider the 24/7 Network under Chapter III, Section 2, Title 3 of the Cybercrime Convention. See also Chapter III, Section 1, Title 1 (on the general principles relating to international co-operation) and Titles 3 to 4 (on the general principles relating to mutual assistance and procedures pertaining to mutual assistance requests in the absence of international agreements) as well as Section 2, Titles 1 to 3 of the Convention.

[203] Note that this may only be appropriate in some cases such as in the case of cyber fraud and identity theft through phishing and similar methods. Such legislation must be carefully drafted so that it is not ambiguous or encounter problems such as an over-incursion into civil liberty rights.

[204] See Chapter II, Section 1, Title 5, Article 13 of the Cybercrime Convention, which states that each party "…shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty…[and] shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions."

system to aid and assist in future investigations and in the development of computer forensics.

9. Technological neutrality – The law should be drafted in such a way as to ensure its applicability to changing technology and techniques used to perpetrate criminal offences as far as possible. If technologically neutral provisions are not possible for a particular subject matter, then fast and reactive amendments or updates to the law are the only other alternative.
10. One-step Recourse – For the sake of clarity, transparency and ease of recourse, legislation directly dealing with computer and cyber crime that are preferably labeled as such and that contains provisions, illustrations and explanatory notes on point will be useful to potential offenders, possible victims and law enforcement officers. This is preferable to a messy and confusing array of different laws that may be applicable such as theft, fraud, identity theft and other legislation.

International connectivity and ease of transacting through information technology is valuable and, if mismanaged, will be squandered as an asset for human progress and interaction. As it is, computer crimes, cyber crimes and other abuses of the Internet, mobile and broadcast networks have damaged the trust and confidence in their use. This has adversely affected the full utility and potential of the cyber realm as another dimension, and the use of electronic media as a means, for humans to communicate and transact. Constant awareness and efforts to manage these resources can and will reverse this trend and reinstate a lawful and orderly cyber society for the benefit of all.

Legal Remedies and Regulatory Challenge

In Malaysia, legal action that can be taken by consumers towards the phisher after realizing the attack is limited. The only existing acts that can be used by consumers are the Computer

Crime Act, Communication and Multimedia Act, Penal Code and Minimum Guideline, also in addition Consumer Protection Act 1999. But this act only focuses on the goods and services that are offered and supplied to consumer in a trade. In Part 1 Section (2) Subsection 2(g), it clearly states that this act shall not apply to any transactions effected by electronic means unless otherwise prescribed by the Minister. Therefore it is a challenge for victims to convict perpetrators whom had steal there personal data via fraudulent schemes.

In 2002, a surprising act was about to be introduced for the consumers data protection known as the Personal Data Protection Act. Unfortunately this act was delayed due to numerous request of exclusion from corporations. This act consist of nine data protection principles covering the collection, use, disclosure, accuracy, retention, access to and security of personal data. If implemented, it will generate a government that officially appoints data protection and will have the power to monitor and enforce compliance, promote public awareness of the law, encourage trade bodies to prepare industry code of practice and corporate with counterparts in foreign countries

The proposal also can be made to Malaysia legal expertise and authority body to enact the law like currently applied in the United Kingdom legislation to protect consumers' privacy does exist. It is known as the Data Protection Act 1999. Under this act consumers' data are protected and the balances between the right of individual and usage of personal information for rightful reasons are highlighted.

In addition, Malaysia legislation also creating the legal framework based on UK Government's Fraud Bill which has been revised to include a new fraud offence that specifically targets the person responsible for phishing attacks. The new offence, which strengthened the current legislation and ease the path of criminal prosecution, covers

phishing acts under "Fraud by False Representation". It clarifies that any person disseminating an email to large groups of people with falsely claiming to be a legitimate financial institution in order to gain access to individuals' personal financial information will be committing an offence

For instance in this Fraud Bill a phisher can be convicted under Section 2, a phisher is in breach if he dishonestly makes a false representation in a bogus email or fake website and intends to gain or cause loss to business or consumer.

Besides that, owning a fraud website and sending spurious email to victim by phishers who intent to commit offences involving frauds also will be charged under Section 6 and Section 7 where else websites are classified as an electronic program and email as electronic data under Section 8. In addition, this bill also includes a clause which will allow for extradition in such cases, a clause which will be useful in prosecuting offenders who operate overseas and whose crimes are not hindered by geographical borders.

Similar legislation is also found in the United States where the state of California became the first state to enact the law addressing to phishing. Consumers in the States are protected under the Personal Data Privacy and Security Act 2005. Possibly with emerge of these acts confidence among consumers can be achieved by confronting phishing issues.

The United States and United Kingdom both successfully added a new legislation in their existing legal framework to fight phishing, in order to protect their e-commerce consumers and sellers online.

Therefore in this case, Malaysia should follow the steps to enforce a specific legislation for the purpose against phishing in this country since the growth of cyber crime in Asia Pacific had increased dramatically. The new regulation should be a valuable tool to account challenges which have arise the Anti- Phishing Act 2005 and also harmonized with other

existing legislations. This is a good first step and will no doubt need to be revisited at some point in the very near future. Even though it is necessary to use legislation as a deterrence, but legislation alone will not stop the increase of phishing attacks. There are some difficulties in convicting a phisher under particular legislation. First, phishing attacks happen very fast that gives crime forensics difficulty in tracing or suspecting the scam. Addition to that identification of fraudulent website before the scam happens is beyond the scope of most security technologies especially for cases that involves international phishers.

Even though Malaysia is still in an infant stage, the government, corporations and consumers could not afford to neglect this approaching and frightening fraud. On the contrary, each party must work hand-in-hand to turn the tide against proliferating fraud. Last but not least, solution for phishing is likely to be a combination effort between education, technology, legislation and law enforcement