AN OVERVIEW OF CYBER SECURITY IN MALAYSIA

Ganesin A/L Supayah
Jamaludin Ibrahim
International Islamic University Malaysia (IIUM), Kulliyyah of ICT, P.O Box 10, Jalan Gombak, 53100-Kuala Lumpur, Selangor, Malaysia
Corresponding e-mail: jamaludinibrahim@iium.edu.my

Abstract
The main aim of this paper is to evaluate the current state of cyber security in Malaysia and to identify the factors which need to be addressed in order to create a secured cyber space. Although the Malaysian government takes various steps to control and protect its cyber citizens, yet the cybercrimes are increasing in line with the number of cyber space users. In this paper, three factors, namely technology, organizational and human factors were identified as the factors governing cyber security protection in Malaysia.

Keywords*:* cyber security, technology, organizational, human, factors, Malaysian government

Introduction

Cyber security refers to "a measure for protecting computer systems, networks, and information from disruption or unauthorized access, use, disclosure, modification or destruction" (Gallaher, Link & Rowe, 2008). Cyber security ought to be an essential part of every Internet users. The borderless and faceless communication creates a lot of security problems for the users. Countries around the world work independently and also through cooperation with other countries to create a safer cyber space. Malaysia is no exception for this. In this conceptual paper, we would like to discuss three factors, which need to be considered in order to enhance the security level in cyber space. We classify the factors as technical, organizational, and human factor. Technology factor refers to the technology that can play a major role in providing protection to the cyber citizen. Technology can be in the form of hardware or software or a combination of both. Organizational factors discuss the role of the Malaysian government in combating cybercrimes and protecting cyber space users. The role of the Malaysian government is discussed in two aspects, namely, the special agency formed by the Malaysian government and the acts enacted by the government. Human factor refers to the users of cyber space.

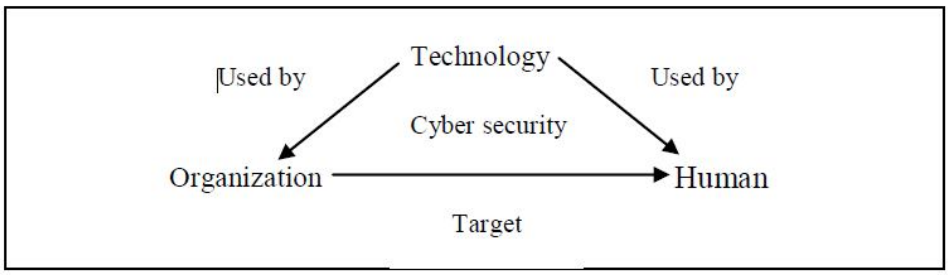

Figure 1: Factors governing cyber security and the relationship between them

Figure 1 illustrates the three factors of governing cyber security and the relationship between them. Generally, technology is used by Malaysian government to protect the cyber users. Malaysian government needs to tackle the human issue in order to prepare an effective cyber security protection plan. At the same time, human could protect themselves using the available technology. The diagram clearly shows that in order to enhance the cyber security protection, the three factors need equal consideration. If one of these factors is not given adequate importance the whole cyber security protection would fail.

Internet Penetration in Malaysia

In 1987, Internet was introduced in Malaysia by the Malaysian Institute of Microelectronic Systems (MIMOS) through its Rangkaian Komputer Malaysia (*RangKom*) project. *RangKom* is an experiment project which was successful in connecting several universities in Malaysia. Later in 1991, *Rangkom* was turned into an Internet Service Provider (ISP), where it was offering services to limited members of public. In the following year, MIMOS launched JARING, Malaysia‟s first ISP (Ali Saman, Mohd Safar Hasim, 2011). As Paynter & Lim (2001) stated, the Internet age in Malaysia began in the year 1995. According to the study conducted by Beta Interactives Services (as cited in Paynter & Lim, 2001), from October to November 1995, it was found that one out of every one thousand Malaysians had access to the Internet, which translated to 20,000 Internet users out of the then total population of 20 million. In 1998, the percentage of Internet users grew up to 2.6% of the total population. After year 2000, Internet penetration in Malaysia continues to grow rapidly.

Table 1: Internet users, total population and the percentage of Internet users in Malaysia.

Year	Internet Users	Total Population	% Percentage
2000	3,700,000	24,645,600	15.0 %
2005	10,040,000	26,500,699	37.9 %
2006	11,016,000	28,294,120	38.9 %
2007	13,528,200	28,294,120	47.8 %
2008	15,868,000	25,274,133	62.8 %
2009	16,902,600	25,715,819	65.7 %
2010	16,902,600	26,160,256	64.6 %

Malaysia shows a rapidly growing number of Internet users, where in 1995, the number of Internet users stood at only 0.1% and within 10 years this grew up to 37.9%. According to the Cyber Security Malaysia, by May 2011, Malaysia has around 17 million Internet users for a population of 28 million people. According to Internet World Stats, Malaysia is at rank 40th in the list of countries with the highest Internet penetration rate. This information is collected for the year of 2009, where Malaysia had an Internet penetration rate of 65.7%. Further, countries with Internet penetration rate of more than 50% only qualified for this list.

The Nielson's Mobile Insights Malaysia 2010 survey reported that the Internet usage in Malaysia has increased up to 41% of subscribers or active users. Consumers in the age group of 20-24 recorded as the highest age group accessing the internet where they are spending an average of 22.3 hours online per week. The survey also stated that the most popular online activities are spent on social networking platform, while instant messaging comes in second at 35%. Furthermore, the study also added that mobility became the key factor in subscribing to a mobile broadband, hence the subscriptions double from 20% in the year 2009 to 54% in the year 2010. User subscriptions for fixed broadband decreased by 23 points to 42%. Dial-up, once the popular method for connecting to Internet has become obsolete with only 2% of subscribers. The survey also reported that laptops and netbooks were widely used by Internet users to access the Internet, with these users accounting for 55%. All the above statistical data shows the rapid growth and evolution of Internet in Malaysia. But there is digital divide between rural and urban areas. Ramasamy in 2004 (as cited in Jeffri bin Idris, Laili bin Hj. Hashim and Aida Wati binti Zainan Abidin, 2011), has reported that Internet subscribers in Malaysia consisted of 93% of urban users. Furthermore in the following literature sources, Alhabshi, Zaitun & Crump, Kementerian Pelajaran Malaysia and Suruhanjaya Komunikasidan Multimedia [SKMM] (as cited in Jefri bin Idris, et al., 2011) also acknowledged the existence of digital inequalities between urban and rural areas in the aspects of access to the computer and Internet.
In the same journal article, the authors acknowledged the efforts taken by government by organize various projects in all levels namely in school, state and federal level, to improve the ICT penetration level in rural areas as well as urban areas. As Ali Saman, et al., (2011) states, the Internet penetration rate in Malaysia shows an increase, with urban areas or major cities like Kuala Lumpur, Johor, and Penang benefited from this increase, while other areas in the country still experienced low Internet penetration rates. According to Salman and *The Malay Mail* (as cited in Ali Saman, et al., 2011), Malaysia has taken a major step in the process of adopting and using the Internet in the country. This can be seen in the various governmental ICT initiatives such as the Multimedia Super Corridor (MSC) and the launching of High Speed Broadband (HSBB). All the above findings obviously show that the Internet penetration is increasing rapidly in Malaysia but is the Malaysian cyberspace fully protected? What is the current state of Malaysian cyber security?

The State of Cyber Security in Malaysia

"Malaysia is one of Asia‟s most alluring countries for cyber criminals. Why? And what is being done by the government to shore up its defenses?" This issue of cyber security has been investigated by Robin Hicks who attended as a speaker in a high-level government conference in year 2010. Furthermore, he stunned his audience of Malaysian civil servants when he showed a slide show with Malaysian government's website which was hacked and festooned with images of

naked woman (Cyber Security Malaysia, 2010). Although the statement was bluntly made, nevertheless the people of Malaysia nor the Government of Malaysia should not deny the poor state of Malaysian cyberspace. Malaysian government efforts go down the drain when Malaysia suffers from more malicious invasions than most countries in the region. In the same article, a Symantec Report produced in February 2010 quoted that 87 percent of all Malaysian web traffic is malware and only 0.2 percent originated from Malaysia to global networks. During a Cyber Security media briefing in 2009, CEO Lt.Col (retired) Husin Haji Jazri, Malaysia‟s leading cyber specialist from Cyber Security Malaysia, said that the cyber security level in the country is above the average and in many instances better compared to other developed countries. He was quoting this based on the effective response mechanisms to cyber threat and that has been planned by the Malaysian authorities. Furthermore, he was saying that the cyber specialist centres are always available for users to report their complaints or any cybercrimes (Cyber Security , 2009). If this is the case, why did Robin Hicks point that our Malaysian cyberspace is a popular target for cyber criminals?

According to statistics collected from Cyber Security Malaysia‟s website, the reported incidents of cybercrime recorded by Cyber999 in Malaysia increased from 3,564 cases in 2009 to 8,090 cases in 2010. The reported cybercrimes increased 127% within one-year period. As of November 2011, the total number of reported cybercrimes was 14,157. This is hard evidence that shows cybercrimes are increasing at an alarming rate. According to Lt Col (Rtd) Prof Datuk Husin Jazri, the Cyber Security Malaysia chief executive officer, until August 2011, there were 10,000 cases reported every month in Malaysia. He added that the Cyber Early Warning System that has been set up by Cyber Security Malaysia detected over 5,000,000 security threats until August this year (Jo Timboung, 2011). Moreover, Sazali Sukardi, during the National ICT Conference, had quoted that according to an article published on 17th April 2008, in the The Star Online, it is estimated that in Kuala Lumpur, there were 99,000 cases of bot-infected personal computers, the highest in the Asia-Pasific region. This makes our capital as the most suitable “honeypot” for hackers. According to the Deputy Minister of Science, Technology and Innovation Datuk Fadillah Yusof, Malaysia will lose RM2.73 billion in the next 5 years if cybercrimes are not properly managed. In 2009 alone, the Malaysian government suffered losses totaling RM22.3 million. For 2010, this increased to RM62 million (“Cybercrimes”, 2011). Based on the preceding statistics, it is obvious that our cyberspace is in a huge mess. If Malaysia does not react now it will be too late and the consequences will be unbearable. It is now or never. What can be done? What are factors that need to address in order to create a secured cyber space for users in Malaysia?

Factors Governing Cyber Security

Based on the statistical information provided in the preceding discussion it is very obvious that Internet penetration is growing rapidly. Also growing is the number of cybercrimes. It is not viable to eliminate cyber security problems totally, yet these cyber security issues need to be addressed properly before it is too late. The three factors that need full consideration in preparing a cyber security plan are: technology factor, organizational factor, and human factor.

Technology factor

Security tools that are available differ in terms of type, number of attacks they address, effectiveness, costs and complexity. Some of these tools were created for single purpose such as

virus scanner and some tools were designed for general purpose, for example intrusion detection and prevention systems. The cyber security tools and activities include firewalls, content filters, intrusion detection and prevention systems, access control, strong user authentication, cryptography, hardening, auditing, end-user and administrator training and insurance (Gallaher, et al., 2008). According to these authors, some of these security tools can be used by both, the attacker and the security administrator but for conflicting purposes. The same technology is also used by the attacker and also security community. Technology becomes a double-edged sword. Furthermore, technology and tools are freely available for both attacker to launch the attacks and security community to detect and defend the system. This fact is also acknowledged by Abu Bakar Munir and Siti Hajar Mohd Yasin (2010), when they said that "Internet is already very helpful for malicious minds who wish to pursue their malicious intention".

Ciampa (2010) stated that managing the security becomes a real challenge since the number of attacks is ever increasing so as the difficulties faced in defending against these attacks. According to him, the tools for attacking any system are readily available and they can quickly scan the systems weaknesses and launch the attack at a very high speed. Besides, attackers launch highly sophisticated and complex attacks using common Internet tools. These types of attacks make the detection and defense more difficult. To make matters worse, the tools to launch these security threats are highly sophisticated and easily available for the attackers and successfully can be used by even an attacker without any technical background. By using the sophisticated tools, the attackers could quickly detect the system vulnerabilities before it is known to the security community. The number of malware or malicious attack programs are produced so rapidly, until software vendors could not produce the needed patches on time to protect the users. Attackers also launch distributed attacks from several sources which make the detection even more difficult. Sometimes the users were asked some security decisions pertaining to their computers where most of these issues were not understood by the common users. Most of the users tend to click "Yes" for most of the questions without understanding its implications.

Most security experts agree that security is indeed a complex problem and it is becoming more complex as the corporate network and business needs progress. But most security professionals also believe that we have the necessary and needed technology to secure even the most complex corporate network (Howard & Prince, 2011). Further these two authors also point out that the complexity and costs involved in managing the Information Technology environment increased as there are more security devices, applications and policies to be managed. Simply said, the number of security initiatives in Information Technology, will lead to increasing the level of complexity and also give negative impact in delivering positive user experience. Besides, they explained that the first 20% of the security spending will provide 90% of the protection needed. The last 80% will just provide small incremental gains, and at the end no one can be 100% secured. They also argued that there will always be evolving threats that would beat even the best security. From the above discussion, the available technology is sufficient to protect the current cyber space. And at the same time the easily available technology enables the attackers to launch the attacks on any systems. But some security experts believe that the systems security failed when it involved the human involvement. To conclude, when the cyber security plan is drafted an organization should consider the human touch into the systems and must ensure that human point is effectively addressed in any cyber security protection plan. The above technology factor is not a local issue but a global issue impacting the whole world, including Malaysia. Everyone is sharing

the technology, information and the security tools. So, there must be a homogeneous solution to address the security using the technology factor.

Organization factor

In this section, we discuss the role of the Malaysian government in combating cybercrimes and protecting cyber space users. The Malaysian government responds to cyber security issues through Cyber Security Malaysia, which reports to the Ministry of Science, Technology and Innovation (MOSTI). Initially, Cyber Security Malaysia was a small department within the Malaysian Institute of Microelectric Systems (MIMOS), a research centre that supports the local IT industry and operates Malaysia‟s Computer Emergency Response Team (MyCERT). Later, with the evolution of the Internet and cybercrimes, this agency was later renamed as National Security Emergency Response Centre (NISER). NISER was given additional capabilities in digital forensics, business continuity and raising cyber security awareness. In 2006, the National Cyber Security Policy (NCSP) was approved. NISER was given the power to implement the policy. The objective of the policy was to make Malaysian IT Systems "secure, resilient, and self-reliant". Later NISER renamed as Cyber Security Malaysia. The agency‟s first move was the Cyber 999 Help Centre, which was set up in July 2009. The general public can report any types of cybercrimes through their website, www.Cyber Security .my. Cyber Security is responsible for designing awareness programs, various types of seminars, training and talk shows for everyone. The Malaysian Government also implements its various initiatives through Cyber Security Malaysia (*History*, 2012). Next, the Malaysian government has passed specific cybercrime laws which are embodied in the following acts: Computer Crimes Act 1997 and Communications Multimedia Act (CMA) 1998. Although the penal code had never been amended to adapt to cyberspace, but occasionally it was used to charge cybercrime criminals (Abu Bakar Munir, et al., 2010). A question to be asked is whether the introduction of the law will govern the cyber space effectively? Many experts believe that law alone cannot secure the cyber space. This is well said by Abu Bakar Munir, et al., (2010, p.132):

According to Moore (2011), the nature of the Internet and the use of Internet, will likely fail the efforts of law enforcement officers in combating the cybercrimes. Enactment of specific acts in law is essential to combat cybercrimes but it could not guarantee full protection to cyber space due to the borderless communication involved. Enforcement officers who are well versed in technology are also one of the requirements to ensure that the law could be enforced successfully. According to Abu Bakar Munir, et al, (2010), in Malaysia, the Malaysian Police Force established a special section under the commercial crime division to deal with cybercrimes. But to tackle the cybercrimes, the enforcement officers need to be technology savvy and they have to be on par with these cyber criminals who are using sophisticated technology to commit the crimes. Another problem in handling these cybercrimes by a nation is this crime is a global phenomenon. Any single nation would not able to combat these crimes without cooperation from the whole world. Meaning, cooperation among nations is necessary to reduce and control these cybercrimes before it becomes out of control. According to Moore (2011), globalization makes the world "shrink" and it makes possible to everyone to share anything, including technological ideas. This globalization phenomenon enables anyone to commit a crime without any physical presence and the prosecuting process of the person who is responsible is impossible as he or she could perform that out of the jurisdiction of that country.

Human factor

From the above two factors, it is obvious that there is a weak point in handling the cyber security using the above mentioned factors alone. This weak point is the cause why most of the time the security set up by corporate organizations failed miserably. The weak point or link in the IT security is the people or the end users themselves. The following quotes acknowledged the fact that human is the weakest link in the IT security. "People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems" (Schneier, 2004, p.255). "7 out of 10 Malaysian adults thought most probably they will be a victim of physical crime rather than a cybercrime." – A survey by Norton Cybercrime in 2011. According to Howard, et al., (2011), people are lack in discipline to enforce the best practices that they learn when they are using computerized Information Systems. People do not set a high priority for security. These authors further argued that the "human and technology touch points are often IT security failures, not the technology." He further elaborates that most of the time technology will operate accordingly. The human element, where the user needs to do something manually in the information systems, will often result in IT or IT security failure. According to Moore (2011), it is important to educate the potential victims regarding the danger of Internet. An example given is identity theft where it is impossible for the enforcement agencies to investigate each and every case. The best solution is the users must aware of the danger and they must be more cautious when using the Internet to accomplish their work.

Conclusion

Creating awareness on cyber security issues is very important for Malaysians as Malaysia is seen as a progressing nation in the field of technology. Usage and popularity of Internet is growing. With this, the concern related to cyber security threats are also increasing. Presently the government takes many initiatives to plan and develop security measures that will be used to protect the cyber users. Still, the number of cybercrimes is ever increasing. As discussed in this paper, all the three factors, namely technology, organizational and human must be considered equally before any cyber security plan is drafted. This is because all the three factors are interrelated. The available technology is used by organization (Malaysian government) to protect the cyber space. Both the technology factor and organizational factor will be effective only if the human factor is taken care of. Failure in handling the human factor, will fail the efforts taken by the Malaysian government in creating a secured cyber space. Considering one factor as more important than the other is not going to solve the current problems related to cyber space. Most of the time Malaysia alone will be unable to draft the security plan based on technology as Malaysia plays the role as a user rather than inventor of technology. On the organizational factor still there is a room for improvement as participation in the global level is required to plan a security plan effectively. Finally for the human factor many aspects need further improvement, as the programmes drafted by Cyber Security Malaysia did not reach the targeted audience. This can be seen from the number of cybercrimes that are sky rocketing in Malaysia.

References

Abu Bakar Munir, Siti Hajar Mohd Yasin. (2010). *Information and Communication Technology Law.* Petaling Jaya: Sweet & Maxwell Asia.

Ali Saman, Mohd Safar Hasim. (2011). Internet Usage in a Malaysian Sub-Urban Community: A Study of Diffusion of ICT Innovation. *Innovation Journal: The Public Sector Innovation Journal*, 16(2), article 6.

Bruce Schneier. (2004). *Secrets and Lies.* Indianapolis: Wiley Publishing Inc.

Bruce Schneier. (2008). *Schneier on Security*. Indianapolis: Wiley Publishing Inc.

Cyber security level in Malaysia better than those in developed countries. (2009).

Cybercrime Investigating high-technology computer crime. Oxford: Anderson Publishing. The Nielsen Company. (2011). *Usage of Internet Increased to 41% with Consumers Aged 20-24 Spending an Average of 22.3 Hours Per Week Online.* Retrieved November 6, 2011 from http://my.nielsen.com/news/20110413.shtml

Cybercrimes may cost nation RM2.73b. (2011, November 11). *The Sun*, p. 9. Sazali Sukardi. (2011, July 7). *Ensuring a safer, stronger digital marketplace – Governance of Online Presence.* Slide show presented at the National ICT Conference Putrajaya. Retrieved December 20, 2011. from apps.intan.my Robert Moore. (2011).

Jeffri bin Idris, Laili bin Hj. Hashim, Aida Wati binti Zainan Abidin. (2011). Digital Inequalities between the rural and urban students in Malaysia. *International Journal of Business and Social Science*, 2(12), 201-208.

Jo Timbuong. (2011). *Cybercrimes continue to rise.* Retrieved November 3, 2011, from http://www.apecdoc.org/site/malaysia/2011/09/26/cybercrimes- continue-to-rise/ Malaysia Vs Malware. (2010).

John Paynter, Jackie Lim. (2001). Drivers and Impediments to E-Commerce in Malaysia. *Malaysian Journal of Library & Information Science.* Retrieved November 20, 2011, from http://umepublication.um.edu.my/filebank/published_article/1849/173.pdf

Malaysia Internet Usage Stats And Marketing Report. Retrieved December 23, 2011, From Http://Www.Internetworldstats.Com/Asia/My.Htm Internet World Stats (N.D.). *TOP 58 COUNTRIES WITH THE HIGHEST INTERNET PENETRATION RATE (OVER 50 PERCENT OF THE POPULATION USING THE INTERNET).*

Malaysians need to increase security awareness. (2011). Retrieved November 6, 2011,from http://www.Cyber Security .my/en/knowledge_bank/news/2011/main/detail/2035/index.html Mark Ciampa. (2010).

Michael P.Gallaher, Albert N.Link, Brent R.Rowe. (2008). *Cyber Security.* Cheltenham: Edward Elgar Publishing Limited.

Retrieved December 23, 2011, from http://www.internetworldstats.com/top25.htm

Retrieved March 20, 2012, from http://www.Cyber Security .my/en/about_us/history/main/detail/734/index.html Internet World Stats (n.d.).

Retrieved October 2011, from http://www.Cyber Security .my/en/knowledge_bank/news/2009/main/detail/1725/index.html Doug Howard, Kevin Prince. (2011). *Security 2020. Reduce Security Risks This Decade.* Indianapolis: Wiley Publishing, Inc. *History*. (2012).

Retrieved October 2011, from http://www.Cyber Security .my/en/knowledge_bank/news/2010/main/detail/1900/index.htm

Security Awareness:Applying practical security in your world. Boston: Course Technology.