An Overview of Cyber Security in Malaysia

[1]Dr. Mamta Bansal,
[1]Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- [1]mamta.bansal@shobhituniversity.ac.in,

ABSTRACT: ***The primary goal of this paper is to assess Malaysia's present status of cyber security and to highlight the elements that must be addressed in order to establish a safe cyber environment. Despite the Malaysian government's efforts to regulate and safeguard its online citizens, cybercrime is on the rise in tandem with the number of people using the internet. Three elements were recognized as controlling cyber security protection in Malaysia in this paper: technological, organizational, and human factors. Malaysian businesses in cybersecurity, as well as to provide a solution for them to solve cybersecurity problems. The information was gathered via interviews with experts in the area of cybersecurity. The findings showed that in order to integrate a cybersecurity aspect in the business, awareness and money are critical. Cybersecurity is beneficial and desirable as a safeguard for an organization's strategic planning in order to improve profitability and production of products and services. This study will be helpful to the business since it will offer a solution to the company's cybersecurity problems. As a result of this study, a business may be able to improve its competitiveness by better understanding the issue and adopting cybersecurity.***

KEYWORDS: ***Cyber Security, Technology, Organizational, Human, Factors, Malaysian Government.***

1. INTRODUCTION

The Internet is among the most advanced technologies ever devised. The Internet and its associated technologies are always changing [1]. The number of Internet users and their reliance on the Internet is constantly growing throughout the world. Malaysians are not immune to the fast development of technology, since their everyday lives are becoming more reliant on the Internet to complete their task. In Malaysia, the number of Internet users is rapidly increasing. According to Muniand (2012), the Internet penetration rate in Malaysia continues to rise quickly after the year 2000. Malaysian Internet users increased from 0.1 percent in 1995 to 37.9% in 2005. The Malaysian Communications and Multimedia Commission (2015) reported that in the first quarter of 2014, Malaysians had a 66.6 percent Internet penetration rate, or roughly 20.1 million Internet users. Cyber security is defined as “a method for preventing interruption or unauthorized access, use, disclosure, modification, or destruction of computer systems, networks, and information” . Cyber security should be a priority for all Internet users [2]. Users confront many security issues as a result of borderless and anonymous communication. Countries all around the globe collaborate to build a safer cyber environment, both individually and in collaboration with one another. This is also true in Malaysia [3].

In this conceptual paper, we will explore three aspects that must be taken into account in order to improve cyberspace security. We divide the elements into three categories: technological, organizational, and human. The technological element refers to the technology that can play a significant part in providing cyber citizen security. Technology may take the shape of hardware, software, or a hybrid of the two. The role of the Malaysian government in fighting cybercrime and safeguarding cyberspace users is discussed in organizational factors. The Malaysian government's involvement is examined from two perspectives: the special agency established by the government and the laws passed by the government [4].

The term "human element" refers to the people who utilize the internet. The three elements that control cyber security, as well as their connection. In general, the Malaysian government employs technology to safeguard cyber users [2]. In order to create an efficient cyber security protection strategy, the Malaysian government must address the human problem. At the same time, humans might use existing technology to defend themselves. The picture clearly illustrates that all three variables must be taken into account in order to improve cyber security protection. If one of these variables isn't given enough weight, the whole cyber security system will collapse.

1.1 Internet Penetration in Malaysia:

The Malaysian Institute of Microelectromechanical System launched the Rangkaian Komputer Malaysia project in 1987, which was the first to bring the Internet to Malaysia. RangKom is a pilot initiative that successfully connected many Malaysian institutions. Rangoon was then transformed into an Internet Service Provider (ISP) in 1991, and it began providing services to a select group of people[3]. MIMOS established JARING, Malaysia's first Internet service provider, the following year. The Internet era in Malaysia started in 1995. According to a survey performed by Beta Interactives Services one out of every 1,000 Malaysians had access to the Internet during October and November 1995, translating to 20,000 Web users out of a total population of 20 million at the time. The proportion of people who use the Internet increased to 2.6 percent of the entire population in 1998. Malaysia's Internet penetration has been steadily increasing since the year 2000. Malaysia has a fast increasing number of Internet users, with just 0.1 percent of the population using the Internet in 1995 and 37.9 percent in ten years. According to Cyber Security Malaysia, Malaysia has approximately 17 million Internet users in May 2011 out of a total population of 28 million people. Malaysia is ranked 40th on the list of countries with the greatest Internet penetration rate, according to Internet World Stats. This data was gathered for the year 2009, when Malaysia had a 65.7 percent Internet penetration rate. In addition, only nations with an Internet penetration rate of greater than 50% qualify for this ranking.

According to the Nielsen Mobile Insight Malaysia 2010 study, Internet use in Malaysia has risen to 41% of subscribers or active users. Consumers aged 20 to 24 are the most likely to use the internet, spending an average of 22.3 hours a week online. According to the study, social networking platforms are the most popular online activity, with instant messaging coming in second at 35%. Furthermore, according to the research, mobility has become a significant element in deciding whether or not to subscribe to mobile broadband, with subscribers increasing from 20% in 2009 to 54% in 2010. Fixed broadband subscribers fell by 23 percentage points to 42 percent [5]. With just 2% of users, dial-up, long the most common way of accessing to the Internet, has become outdated. According to the study, laptops and netbooks were extensively utilized by Internet users to access the Internet, accounting for 55% of all users. All of the following statistics demonstrate the Internet's fast development and evolution in Malaysia. Rural and urban regions, however, have a digital gap. According to Ramasamy, 93 percent of Internet customers in Malaysia are urban. Furthermore, Alhabshi, Zaitun & Crump, Kementerian Pelajaran Malaysia, and Suruhanjaya Komunikasidan Multimedia [SKMM] acknowledged the existence of digital inequalities between urban and rural areas in terms of access to computers and the Internet in the following literature sources. The authors of the same journal article praised the government's efforts to increase ICT penetration in rural and urban regions by organizing different initiatives at all levels, including school, state, and federal levels. According to the Internet penetration rate in Malaysia is increasing, with metropolitan regions or large cities such as Kuala Lumpur, Johor, and Penang benefiting from the rise, while other parts of the nation continue to have low Internet penetration rates. According to Salman and The Malay Mail, Malaysia has progressed significantly in its adoption and use of the Internet. Various government ICT efforts, such as the Multimedia Super Corridor (MSC) and the introduction of High Speed Broadband, demonstrate this (HSBB) [6].

1.2 The State of Cyber Security in Malaysia:

For cyber thieves, Malaysia is one of Asia's most appealing nations and what is the government doing to strengthen its defenses. Robin Hicks, who spoke at a high-level government meeting in 2010, looked into the subject of cyber security. He also shocked his Malaysian civil servant audience when he presented a slide show of the Malaysian government's website, which had been hacked and was strewn with pictures of nude women Security Malaysia. Despite the bluntness of the remark, neither the Malaysian people nor the Malaysian government should deny the terrible condition of Malaysian interne t[7]. Malaysian government attempts are futile since the country is subjected to more malevolent incursions than the rest of the area. According to the same article, a Symantec report published in February 2010 said that 87 percent of all Malaysian online traffic is malware, with just 0.2 percent of all Malaysian web traffic originating from Malaysia to worldwide networks. In 2009, at a Cyber Security media conference, CEO(retired), Malaysia's top cyber expert from Cyber Security

Malaysia, said that the country's cyber security level is above average and, in many cases, better than other developed countries. He was citing efficient cyber threat response measures that Malaysian authorities had devised. Furthermore, he said that the cyber expert centers are always open for people to report any cybercrimes or concerns [8]. If that's the case, why did Robin Hicks say that internet in Malaysia is a favorite target for cyber criminals?

According to information gathered from Cyber Security Malaysia's website, the number of reported cybercrime events in Malaysia rose from 3,564 in 2009 to 8,090 in 2010. Within a year, the number of recorded cybercrimes rose by 127 percent. The overall number of recorded cybercrimes was 14,157 as of November 2011. This is concrete proof that cybercrime is on the rise at an alarming pace. According to Cyber Security Malaysia's chief executive officer, Lt Col (Rtd) Prof Datuk Husin Jazri, there were 10,000 instances reported per month in Malaysia till August 2011. He went on to say that till August of this year, Cyber Security Malaysia's Cyber Early Warning System has identified over 5,000,000 security threats. Furthermore, at the National ICT Conference, Sazali Sukardi said that according to an article published in The Star Online on April 17, 2008, it is believed that there were 99,000 instances of bot-infected personal computers in Kuala Lumpur, the most in the Asia-Pacific area. As a result, our capital is the best "honeypot" for hackers. Malaysia would lose RM2.73 billion in the next five years if cybercrime is not effectively handled, according to Deputy Minister of Science, Technology and Innovation Datuk Fadillah Yusuf. Malaysia's government incurred losses totalling RM22.3 million in 2009. This rose to RM62 million in 2010. Based on the data presented above, it is clear that our cyberspace is in shambles [9].

1.3 Factors Governing Cyber Security:

It is clear from the statistical data presented in the previous section that Internet penetration is quickly increasing. The number of cybercrimes is also on the rise. Although it is impossible to completely eradicate cyber security concerns, these issues must be handled before it is too late. Technology, organizational, and human aspects are the three elements that must be fully considered while creating a cyber-security strategy [10].

Technology factor: The types of security tools available vary in terms of their effectiveness, cost, and complexity, as well as the number of attacks they address. Some of these tools were created for a specific purpose, such as virus scanners, while others, such as intrusion detection and prevention systems, were created for a general purpose. Firewalls, content filters, intrusion detection and prevention systems, access control, strong user authentication, cryptography, hardening, auditing, end-user and administrator training, and insurance are among the cyber security tools and activities (Gallaher, et al., 2008). Some of these security tools, according to these authors, can be used by both the attacker and the security administrator, but for opposing purposes. The attacker and the security community both use the same technology. Technology has the potential to be a double-edged sword. Furthermore, both attackers and the security community have free access to technology and tools to launch attacks and detect and defend the system. Abu Bakar Munir and Siti Hajar Mohd Yasin (2010) acknowledged this when they stated, "Internet is already very helpful for malicious minds who wish to pursue their malicious intention." According to Ciampa (2010), managing security has become a real challenge because the number of attacks is increasing, as are the difficulties in defending against them. He claims that the tools for attacking any system are readily available, and that they can quickly scan the system for flaws and launch an attack at a high rate.

Furthermore, attackers use common Internet tools to launch highly sophisticated and complex attacks. These attacks make it more difficult to detect and defend against them. To make matters worse, the tools used to launch these security threats are highly sophisticated and easily accessible to attackers, and they can be successfully used even by someone with no technical background. The attackers could quickly detect system vulnerabilities using sophisticated tools before they were discovered by the security community. The number of malware or malicious attack programs is increasing at such a rapid rate that software vendors are unable to provide timely patches to protect users. Attackers often use several sources to conduct dispersed assaults,

making identification even more difficult. Users were sometimes asked to make security choices about their computers, with the majority of these problems being beyond the comprehension of the average user. The majority of users tend to answer "Yes" to most queries without fully comprehending the consequences. Most security experts believe that security is a complicated issue that is only becoming more complicated as corporate networks and business requirements evolve. The last 80% will only offer modest incremental improvements, and no one can be completely secure in the end. They further claimed that changing threats will always outsmart even the greatest protection. According to the debate above, existing technology is enough to defend the current cyber environment. At the same time, attackers may start assaults on any system thanks to readily accessible technologies. However, some security experts think that when humans were engaged, the system's security collapsed. To summarize, while drafting a cyber-security strategy, a company should consider the human touch in the systems and guarantee that the human aspect is handled properly in any cyber security protection plan. The aforementioned technological element is a worldwide problem that affects the whole globe, including Malaysia. Everyone is exchanging information, technology, and security tools. As a result, a unified approach to handle security utilizing the technology element is required.

Factor of organization: The role of the Malaysian government in fighting cybercrime and safeguarding cyberspace users is discussed in this section. Cyber Security Malaysia, which reports to the Ministry of Science, Technology and Innovation, is the Malaysian government's response to cyber security problems (MOSTI). Cyber Security Malaysia began as a tiny section inside the Malaysian Institute of Microelectric Systems (MIMOS), a research institute that supports the local IT sector and houses Malaysia's Computer Emergency Response Team (MyCERT). Later, as the Internet and cybercrime evolved, this organization was renamed the National Security Emergency Response Centre (NISER). Digital forensics, business continuity, and increasing cyber security awareness were all added to NISER's capabilities. The National Cyber Security Policy (NCSP) was adopted in 2006. The policy's implementation was delegated to NISER. The policy's goal was to make Malaysian IT systems "safe, robust, and self-sufficient." NISER was renamed Cyber Security Malaysia afterwards. The Cyber 999 Help Centre, which opened in July 2009, was the agency's first relocation. Through their website, www.Cyber Security.my, the general public may report any kind of cybercrime. Cyber Security is in charge of creating public awareness campaigns, as well as different kinds of seminars, training, and discussion shows. Malaysia's government also uses Cyber Security Malaysia to carry out its different projects (History, 2012).

Following that, the Malaysian government enacted specialized cybercrime legislation, which is enshrined in the following acts: The Communications Multimedia Act (CMA) of 1998 and the Computer Crimes Act (CCA) of 1997 both apply to computer crimes. Despite the fact that the penal law had never been changed to accommodate online, it was sometimes utilized to prosecute cybercrime perpetrators (Abu Bakar Munir et al., 2010). One issue to consider is whether the law's implementation will effectively regulate cyberspace. Many experts think that the legislation alone will not be enough to protect the cyberspace. Abu Bakar Munir, et al., (2010, p.132), put it succinctly According to Moore (2011), the nature of the Internet and how it is used will most certainly fail law enforcement officials' attempts to fight cybercrime. The enactment of particular acts of legislation is necessary to fight cybercrime, but owing to the international communication involved, it cannot ensure complete cyberspace security. One of the prerequisites for ensuring that the law is effectively implemented is for enforcement agents to be well-versed in technology. According to Abu Bakar Munir et al. (2010), the Malaysian Police Force set up a specific department within the commercial crime division to deal with cybercrime. However, in order to combat cybercrime, law enforcement personnel must be technologically knowledgeable and on par with cyber criminals who use sophisticated technology to conduct crimes. Another issue with a nation's management of cybercrime is that it is a worldwide phenomenon. Without global collaboration, no one country would be able to fight these crimes. To put it another way, international collaboration is required to minimize and manage cybercrime before it spirals out of control. Globalization, according to Moore (2011), causes the globe to “shrink,” allowing anybody to exchange anything, including technical ideas. This globalization phenomena allow anybody to commit a crime without having to be

physically there, and prosecuting the perpetrator is difficult since he or she may do it outside of the nation's jurisdiction.

- *Human factor*: It is clear from the above two considerations that managing cyber security only on the basis of the above two elements has a flaw. This flaw is the reason why corporate security systems often fail badly. The humans or end users themselves are the weak point or link in IT security. The following quotations recognized that the weakest link in IT security is the human. "People are often the weakest link in the security chain, and they are constantly to blame for security system failures" (Schneier, 2004, p.255). "More than seven out of ten Malaysian people believe they will be victims of physical crime rather than cybercrime." - Norton Cybercrime conducted a study in 2011. People, according to Howard, et al., (2011), lack the discipline to follow through on the best practices they learn while utilizing computerized Information Systems. People do not place a great value on security. These writers went on to say that "IT security problems, not technology, are typically human and technology contact points." He goes on to say that most of the time, technology will work as expected. When a user has to perform anything manually in an information system, the human factor frequently leads to IT or IT security failure. Moore (2011) believes that it is critical to educate prospective victims about the dangers of the Internet. Identity theft is an example where law enforcement authorities are unable to investigate each and every instance. The greatest remedy is for consumers to be aware of the risk and to be more careful while utilizing the Internet to do tasks.

2. DISCUSSION

Despite the growing importance of cyber-security in security politics and the threat of a large, systemic, catastrophic event affecting key infrastructures, computer network vulnerabilities remain mostly a commercial and espionage issue. Disruptive events in the future, depending on their (possible) intensity, will continue to feed military debate, as well as concerns of strategic cyber-war. Worst-case scenarios are certainly a valid job for the national security apparatus to consider (and prepare for). However, they should not be given undue weight in the face of more realistic and probable issues. The challenge for decision-makers in establishing a sensible strategy is navigating the rough shoals between frenzied apocalyptic predictions and ignorant complacency. Threat-representation must stay well-informed and balanced in order to avoid over-reactions with excessive costs and unclear rewards. An 'arms race' in cyberspace, for example, predicated on fear of other nations' cyber-capabilities, would almost certainly have disastrous consequences for how humanity utilizes the Internet.

3. CONCLUSION

Seeing as Malaysia is regarded as a technologically advanced country, raising awareness about cyber security issues is critical. The popularity and use of the Internet is increasing. As a result, there is a growing concern about cyber security threats. The government is currently undertaking a number of initiatives to plan and develop security measures that will be used to protect cyber users. Despite this, the number of cybercrimes continues to rise. As discussed in this paper, before any cyber security plan is drafted, all three factors, namely technology, organizational, and human, must be taken into account equally. This is due to the fact that all three variables are intertwined. Organizations (such as the Malaysian government) use available technology to protect cyberspace. Only if the human factor is addressed will both the technological and organizational factors be effective. The Malaysian government's efforts to create a secure cyber space will be thwarted if it fails to deal with the human factor. Considering one factor to be more important than the other will not solve the current cyberspace issues. Malaysia will most likely be unable to draft a security plan based on technology on its own because it is more of a user than an inventor of technology. On the organizational level, there is still room for improvement, as global participation is required to effectively plan a security plan. Finally, many aspects of the human factor require improvement, as Cyber Security Malaysia's programs failed to reach the intended audience. The number of cybercrimes in Malaysia is increasing at an alarming rate.

REFERENCES

[1] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[3] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, 2016, doi: 10.1016/j.dss.2016.02.012.

[4] M. Sonntag, "Cyber security," 2016, doi: 10.2478/hjbpa-2019-0020.

[5] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Computers and Security*. 2016, doi: 10.1016/j.cose.2015.09.009.

[6] W. H. Dutton, "Fostering a cyber security mindset," *Internet Policy Rev.*, 2017, doi: 10.14763/2017.1.443.

[7] J. Jain and P. Ram Pal, "A Recent Study over Cyber Security and its Elements," *Int. J. Adv. Res. Comput. Sci.*, 2017.

[8] J. Shin, H. Son, R. Khalil Ur, and G. Heo, "Development of a cyber security risk model using Bayesian networks," *Reliab. Eng. Syst. Saf.*, 2015, doi: 10.1016/j.ress.2014.10.006.

[9] I. Atoum and A. Otoom, "Effective belief network for cyber security frameworks," *Int. J. Secur. its Appl.*, 2016, doi: 10.14257/ijsia.2016.10.4.21.

[10] R. Buch, D. Ganda, P. Kalola, and N. Borad, "World of Cyber Security and Cybercrime," *Recent Trends Program. Lang.*, 2017.