Educating the general public on Cyber-security survival

Mohamed Warsame Omar[1], Naser Yaqubi[2], Jamaludin Ibrahim[3]

[1, 2 3] Kulliyyah of Information and Communication Technology

Authors Email Id: Warsame.omar@live.iium.edu.my [1], naseryaqubi@live.iium.edu.my [2],

International Islamic University Malaysia (IIUM)

Abstract: **In this of era of internet and digital advancement where technology has made the human more dependent on it, almost every family member owns a piece of digital equipment such as laptop smartphone or tablet, Technology has made humans so dependent on it that we feel paralyzed without it, technology has come with it is up's and down's, some of it is implications are how the internet services significantly impacts our Privacy and security whether it is on national level, institutional level or personal level we are all vulnerable when we are talking about this topic of cyber security. Computers and the internet bring many benefits to small businesses, but this technology is not without risks. So many organizations need to invest in there cybersecurity systems in order to be save, such implements an awareness and training programs for their employees. Even Parents are struggling to overcome these negative impacts in relation to their children's technology and internet usage. Technology is rapidly evolving in a world driven by social networks, online transactions, and cloud computing and automated processes. But with the technological evolution comes the progress of cyber-crime, which continuously develops new attack types, tools and techniques so in recent years cyber-security is considered one of the key national security issues due to advancement of technology and internet connectivity. (Bendovschi , 2015) The main objective of this white paper is to propose the practical strategies for educating the general public to be aware of these security threats and now how they can overcome these challenges as long as we are a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyber-attacks. Therefore, protecting it is of paramount priority to protect our information and data. (ACS, 2018).**

Keywords: **Cyber security, Threats, Challenges, business, government, personal information, cyber-attack, cybercrime.**

I. INTRODUCTION

Although technology has become necessary for our daily live in organizational and individual level thus there is so many threats to the security of our information, Cyber security education is a necessary need across all disciplines and majors. (Meso, Ding, & Xu, 2014). Because of the cybercrime increasing now it is very important to know how to secure businesses, enterprises and organizations everywhere, and to understand what can be done to safeguard and protect the confidentiality, integrity and availability of their information assets. (Green, 2013). To help employees recognize and change their computing security behavior, organizations need to invest in cybersecurity training and awareness programs to encourage their employees' active engagement in complying with their security policies (He & Zhang, 2019). Also for the individual to know how his data can securely being transmitted or sent to the other person safely without any leakage of information. It is clear that nowadays cybercrime has become so popular and also the skills of the hackers are increasing rapidly. There is a broad consensus on the need for broader and better training and education of the current and future workforce to be able to effectively deal with present, emergent and future cyber security challenges (Meso, Ding, & Xu, 2014). Cybersecurity is not just about protecting information anymore (Gartner, 2018). Because of these new emerging technology of IoT and AI which will enable self-driving cars now cybersecurity will also be protecting about lives. Currently, Intelligent Things which combine artificial intelligence (AI) and IoT are being developed. Most of these devices are configured to collect and respond to human behavior (motion, voice, etc.) through built-in sensors. If IoT devices do not ensure high security, personal information could be leaked. (Park, Oh, & Lee, 2019). Worldwide spending on information security products and services will reach more than $114 billion in 2018, an increase of 12.4 percent from last year, according to the latest forecast from Gartner, Inc. In 2019, the market is forecast to grow 8.7 percent to $124 billion, Gartner forecasts $124 billion on cybersecurity spending alone in 2019. (Gartner, 2018). As the number and frequency of cyber-attacks designed to take advantage of unsuspecting personnel are increasing, the significance of the human factor in information security management cannot be understated. In order to counter cyber-attacks designed to exploit human factors in information security chain, information security awareness with an objective to reduce information security risks that occur due to human related vulnerabilities is paramount. (Abawajy, 2012) .

II. CYBER SECURITY AWARENESS CAMPAIGN AND SAFEGUARD MECHANISMS

The aim of this awareness campaign is to give cybersecurity awareness presentation and seminars both in organizational and individual level just to enlighten and to give them the attention to recognize IT security concerns and respond accordingly. Today more than 60 percent of total commercial transactions are done online (Bada, Sasse, & Nurse, 2013). Researchers from the Royal Institute of International Affairs concluded that many business executives lack the understanding of cyber threats needed to protect their organizations properly (Green, 2013), To help employees recognize and change their computing security behavior, organizations need to invest in cybersecurity training and awareness programs to encourage their employees' active engagement in complying with their security policies (He & Zhang, 2019). So this field requires a high quality of security for transparent and best transactions so it is crucial to make an awareness and training program for the employees and also managers of those companies. Even all the latest technologies like E-commerce, Mobile computing, cloud and grid computing and Net banking needs high level of security. Training of IT staff working in healthcare settings is of high priority in order to enforce the knowledge on information security processes and data protection procedures(Rajamaki, Nevmerzhitskaya, & Virag, 2018). All over the world government is giving main focus on cyber security and they are giving awareness to peoples how to use different latest technologies and social media. According to current survey in this real world we have millions of cyber-crimes daily (Khan & Haque, 2017). The primary purpose of cyber security-awareness campaigns is to influence the adoption of secure behavior online. However, effective influencing requires more than simply informing people about what they should and should not do: they need, first of all, to accept that the information is relevant, secondly, understand how they ought to respond, and thirdly, be willing to do this in the face of many other demands (Bada, Sasse, & Nurse, 2013).

III. GIVING THE GENERAL PUBLIC AN AWARENESS ON CYBER ETHICS

Cyber Ethics aims at giving orientation and understanding about right and wrong, good and bad, related to the cyber space. It tries to apply and modify fundamental values and virtues to specific new challenges and situations arising from cyber technologies and cyber society. As cyber space influences all parts of society, cyber ethics includes almost all ethics domains (Stückelberger & Duggal, 2018). First in order for you to be protected you should comprehend what is right and what is wrong, you should also know what the risk is. Although there are so many internal and external threats to our data and networks, computer ethics should be concern to everyone. (Gunarto, 2004). For the person to be well aware of these security threats and how to flow the cyber ethics there are good chances for him or her to end up safe. There are so many motivations for users in cyberspace for using and abusing it, some of these motivations are predominantly ethically positive or negative, a good number of them can lead to constructive and destructive results as is the case for many human actions and many human made technologies. (Stückelberger & Duggal, 2018), in this cyber world people should respect the right of the ownership and software usage, they should also protect the privacy of the data about individuals. Individuals constantly prefer to receive to another advancements by disregarding what security issues they can bring to them yet it is likewise significant for you to consistently keep up pace with these new safety efforts that these new technologies require. Another significant risk is the expansion of the more skilled hackers who are more roused than any time and will utilize each system accessible to them. Also there are so many simplified tools and software's that are easy to use which enable unskilled hackers to use them. Social Media Maximum number of users are not aware of the risks and share their information unknowingly and their lack of knowledge makes them vulnerable to cyber-attacks. Danger is always present in Social Media, cyber bullying is another form of crime in the virtual world. It is a deceptive character because of its unidentified style. The cyber bullying is similar to the traditional bullying, (Shuriye&Ajala, 2014) without knowing such dangers and even when knowing, also a person can disguise himself/herself in many different was and can showcase a totally opposite or incorrect personality online convincing the other party. And also may use their items in an appropriate way, this can hurt the recipient party, (Hosseini & Ramchahi, 2014), people should always be ethical and know to respect the other people's feelings. To conclude, ethics has been an integral part of human civilization, human behavior, human conduct and human legislative approaches. Cyber ethics will continue to play increasingly important role for all stakeholders at local, national, regional and international levels to guide various activities of different stakeholders in a positive ethical direction (Stückelberger & Duggal, 2018).

IV. CYBER PARENTING

An Internet connection has become almost ubiquitous in homes with school-age children in developed societies. The Internet is both a great social and learning tool and full of potential dangers. Without proper parental support and guidance, the chances of children being exposed to these dangers increase. Yet this can cause tension and distress between parents and children (Wong, 2010). Internet services significantly impact our Privacy and security especially for our children who are the most vulnerable category when we are talking about this topic of cyber security. Parents seem helpless in struggling to overcome these negative impacts in relation to their children's technology and internet usage. Children, young people and young adults may be better aware of some of the risks that they face online than are adults. Effective strategies thus require their active involvement as actors in their own right to understand their use of information and communication technologies, their awareness of the risks and hazards, and the strategies that they have developed to counter such risks (Stückelberger & Duggal, 2018). For elementary students, security and privacy education is anticipated to be more joyful when the knowledge is delivered in the form of a digital game-based learning activity. This mobile application is for educating and raising young learners' awareness on basic cyber security and privacy issues. (Giannakas, papsalouros, Kambourakis, & Gritzalis, 2019) And the main objective is to provide a good foundation for students in cyber security knowledge and skills, Enhance students' ability to behave in a secure manner online as well as to secure their environment, and Increase their interest in cyber security education. (Peker & Fleenor, 2019).

V. EDUCATING EMPLOYEES AND USERS ON CYBER SECURITY AND SOCIAL ENGINEERING

Consequently, providing technical solutions is not enough. It is important to also enhance training and make provisions for raising the awareness of employees and computer users about how to manage and secure their information online. The user's errors related to technology use cannot be solved by increasing technical tools alone, but an awareness training program can yield excellent results. (Amankwa, Loock, & Kritzinger, 2015). Cyber security is a fast growing discipline and there is a need for more educated and trained personnel who have a mastery of the subject matter. Organizations need to take a strategic role in preparing their workforce and the need for cyber security specialties is one such strategy (McCormick, 2018). Today, organizations are greatly dependent on information systems. This reliance has led to being vulnerable to information security threats that put systems at risk. Furthermore, social engineering fraud has been rising significantly with advancements in technology. Criminals are getting more sophisticated in finding new ways to attack. As a result, organizations have been increasing their investments in cyber security initiatives to safeguard their data (Skinner & Aldawood, 2018). And the aim of educating employees on cyber security is to build employees' skills and appreciation of problem solving, critical thinking, and the ability to handle unfamiliar situations and problems (McCormick, 2018)

VI. CYBER GOVERNANCE A HIGHER EDUCATION CYBER SECURITY CURRICULUM

In order to increase the number of cyber security professionals it is the duty of educational leadership and information technology practitioners to Develop solutions to the challenge of cyber security. The higher education cyber security training curriculum project aligns with the field of educational leadership and management in its focus on dealing with threats that organizations and individuals are exposed to when they embrace advanced technological systems and solutions such as the internet. This will contribute to the reduction in the number of threats that the organizations are exposed to as they leverage new technology and the internet to improve the efficiency of their systems and processes (McCormick, 2018).

At this period of technological advancement where these new technologies bring such a large number of tremendous social activities going through the internet and cyber world. technology has made people so reliant on it that we feel incapacitated without it, the blast of the number of associated gadgets, and the quick take-up of technology, for example, cloud computing, Artificial intelligence (AI) and advanced robotics are essentially changing individuals' lives additionally these new technologies are changing how associations do business and the manner in which governments give public service to the citizens. Moreover educating people on Cyber security is very necessary but sometimes even though people know the safety guidelines tend to give no attention on the consequences of violating these security measures while using the internet and also some other people deliberately steal other people's information in unauthorized way. Therefore in this world of increasing risk there is most need for the governments to draw clear boundaries and regulations in order to combat these Cyber-crimes.

VII. CONCLUSION

Attackers are now using more sophisticated techniques to target the systems. Individuals, small-scale businesses or large organization, are all being impacted. So, all these firms whether IT or non-IT firms have to understood the importance of Cyber Security and focus on adopting all possible measures to deal with cyber threats. As the amount of information, critical services, and interconnected computers in the cyberspace is steadily increasing, the number, sophistication, and impact of cyber-attacks are becoming more and more significant. In the last decades, governmental and non-governmental organizations have become aware of this problem. However, the existing of cyber security workforce has not been sufficient for satisfying the increasing demand for qualified cyber security professionals, and the shortfall will increase in the next years. Meanwhile, to address the increasing demand for cyber security professionals, related governmental institutions have to establish cyber security programs, particularly, cyber security awareness campaigns to the general public in order to enlighten them the security measures that they have to take in order to safe their life's from these cyber-attacks. In this paper we strongly suggest that in this era of digital advancement it is very necessary for every institution to consider this upcoming threats and take the necessary security measures before it is too late.

REFERENCES

[1] Bendovschi. A (2015). Cyber-attacks – trends, patterns and security countermeasures

[2] ACS (2018). Cyber security threats, challenges and opportunities

[3] Meso. P; Ding. Y; Xu. Sh (2014). Applying Protection Motivation Theory to Information Security Training for College Students. *Journal of Information privacy and security*. Volume 9. 2013 – Issue 1

[4] Green. J (2013). Cybersecurity and information assurance. *Prolinx White paper*

[5] He. W; Zhang. Z (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of organizational computing and electronic commerce. https://doi.org/10.1080/10919392.2019.1611528*

[6] Gartner (2018). The 2018 2019 Cyber trends

[7] Park. M ; Oh. H & Lee. K (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. *Sensor MDPI*

[8] Abawajy. J (2012). User preference of cyber security awareness delivery methods. Journal of behaviour and information technology. Volume 33, 2014 - Issue 3.

[9] Bada. M; Sasse. M. A & Nurse J. R (2014). Cyber Security Awareness Campaigns Why do they fail to change behaviour?. *Global cyber security capacity Centre*

[10] Rajamaki. J; Nevmerzhitskaya.J & Virág. C (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF). *DOI: 10.1109/EDUCON.2018.8363488*

[11] Khan. M ; Haque. Sh (2017) Cyber security ethics on social media. *Journal of Modern Developments in AppliedEngineering & Technology Research.*

[12] Gunarto. H (2004). Ethical Issues in Cyberspace and IT Society.

[13] Stückelberger. Ch & Duggal. P (2018). Cyber ethics 4.0 serving humanity with values.

[14] Shuriye. O. A; Ajala. M (2014). Islam and the cyberworld. DOI: 10.5901/jesr.2014.v4n6p513

[15] Hosseini, S. E., Ramchahi A. A.(2014). The Impact of Information Technology on Islamic Behaviour, *Journal of Multidisciplinary Engineering Science and Technology (JMEST*) ISSN: 3159-0040 Vol. 1 Issue 5, December – 2014.

[16] Wong. Y. Ch (2010). Cyber-Parenting: Internet Benefits, Risks and Parenting Issues. *Journal of technology in human service.* Volume 28, 2010 – Issue 4.

[17] Giannakas. F (2019). A comprehensive cyber security learning platform for elementary education. *Journal of information security*. Volume 28, 2019 – Issue 3.

[18] E. Amankwa, M. Loock, and E. Kritzinger (2015 (Amankwa, Loock, & Kritzinger, 2015)). A conceptual analysis of information security education, information security training and information security awareness definitions, in Proc. 9th Int. Conf. Internet Technology and Secured Transactions (ICITST ’14), London, UK, 2014, pp. 248–252.

[19] Alwadood. H & Skinner. G (2018). Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review. *IEEE TALE Conference 2018At: Wollongong, NSW, Australia*

[20] McCormick. B (2018). Higher Education Cyber Security training curriculum.