International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies

M. Abdalla, Y. Arshad
Department of Technology Management,
Faculty of Technology Management and Technopreneurship,
Universiti Teknikal Malaysia Melaka, Melaka,
Malaysia

***Abstract*— As information systems and cyberspace upsurge in complexity and volume, cyber-threats are increasing rapidly, as a result businesses are facing larger security risks in cyberspace in recent times [1]. Cybercrimes have considerably risen for the last decade in Malaysia due to inadequate law enforcement resources being provided to cope with these crimes. In order to secure cyber assets organizations need to communicate technical and behavioral solutions to their employees since the human factor has been considered the weakest line in the defense system or at least it plays a critically significant part in securing cyber systems [2]. Therefore, the aim of this study is to investigate factors influencing the adoption of cyber security standards among Malaysian public listed companies. The study used TAM and DOI models to determine cyber security standard's adoption factors including technological factors, organizational factors and individual factors. The findings indicate that perceived ease of use and expected related benefits are the two main variables in explaining cyber security standard's adoption. This in turn, helps Malaysian public listed companies in bursa Malaysia to obtain a clear picture the key contributors to combat the menace, and avoid sever data breaches and financial impacts.**

Keywords*— *Cybercrimes; cybersecurity; human factors; business aspects;

I. NTRODUCTION

Cybersecurity is one of the major components aspects of national and international security today globally. Studies have shown that over 25 percent of business organizations in Malaysia have faced cyber-attacks that had financial impacts of more than RM 4 billion [3]. As reported by Cisco, cyber-attacks cost financial impacts including lost revenue, loss of clients, and potential opportunities. According to Malaysian Public Listed Companies, cyber incidents tend to negatively affect their stock values. Therefore, to secure cyber assets Malaysian Public Listed Companies need to communicate technical and behavioral solutions to their employees since the human factor has been considered the weakest line in the defense system or at least it plays a critically significant part in securing cyber systems. If employees are not willing to accept cybersecurity standards, IS will not bring the full benefits of the technology to the Malaysian public listed companies [4].

Cybersecurity assists to reduce threats and cyber-attacks that can harm organizations' assets such as software, hardware, or data, and people where should be adhered to by the employees [5]. The terms used for security changed over time as information security professionals modify the term information security to cybersecurity governance the outline eventually overflowing to the public domain, comprising cybersecurity specifically addressing electronic aspects. Yet, the objectives have always been the same which is to primarily protect information or data within the organizations. Based on this observation this research focuses on the factors influencing cybersecurity standard's adoption in MPLCs [6].

As businesses have chosen to use cyber-based platforms in trying to connect to the globe, an immense amount of information is established and adapted it into digital setup. Currently, organizations have recognized their dependence on this infrastructure in their target to achieve their stated cybersecurity, goals and missions and strategic positioning necessary for successful leverage. Yet, in the face of the reality expressed on the need to spend less on IS, and to see it as rather a utility [7]. This information travels across the world via an excessive amount of interconnected networks, which is exposed to cyber threats including spams, phishing malware, Trojans, viruses and other forms of cyber-attacks [8]. However, Effective cybersecurity management cannot succeed without considering the roles of employees in the organizations, studies have shown that cybersecurity incidents from inside can have serious consequences on the computer systems where an employee in the company could cause serious harms fewer efforts and time in accessing the targeted information in comparison to external attacker [9].

II. LITERATURE REVIEW

A. Cyber security standards

Cybersecurity standards have been established to secure organization's cyber assets. Cybersecurity practices and standards are commonly useful for all organizations, regardless of their industry, sector or size [10]. Several attempts have been made to examine the adherence of cyber security procedures. However, it is crucial to study cyber security standards nationally and internationally as shown in figure 1, to have a clear picture about cyber security polices [11].

Over all standards, whether it is a technical standards accountability standards or cyber security standards indicate a set of requirements that system or data must achieve. In assumption of accordance of certain system with particular standards

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

illustrates that it fulfills all the standard's stipulations. Implementing standards is universally accepted and provides the likelihood of comparing a personal security system with a given frame of reference adopted at an international level [12].

Cyber security standard's adherence implementation in Malaysia is supported by the (NCSP). The Malaysian National Cyber Security Policy seeks to strengthen the country's critical national cyber infrastructure and facilitate the country's drive towards more secure systems and cope with cyber security crises [13].

Table 2.1: Cyber security standards inventory (Source: Hulsebosch et al. , 2015)

Title	Source	Origin	Language	type	Vital sector
ISO/IEC 27002	ISO/IEC	International	English	Standard	General
ISO/IEC 27001	ISO/IEC	International	English	Standard	General
NERC CIP 002-009	NERC	International	English	Standard	Energy
NIST SP-800 series	NIST	USA	English	Guideline	General
ISA/IEC 62443	ISA	USA	English	Framework	Industry
AGA No.12	AGA	USA	English	Best practices	Telecommunications
COBIT5	ISACA	International	Multiple	Method	General

B. Cyber security in Malaysia

Malaysia considers one of the most seducing countries for cyber attackers. The form of data breaches are in continues evolvement, butting Malaysian business aspects under cybercrimes. Therefore, lot of efforts have been made to establish safety and security for the cyberspace including Malaysia by referring to the technology where it could be combination of both software and hardware in order to cope the cyber risk and overcome it since the technology plays ultimate part in offering security to business enterprises[14]. As the information systems become more advance and multifaceted the level of vulnerability will rise [15]. The growth of cyber security strategies is essential step toward formulating Malaysian listed companies against any internal or external threat sources where managerial strategies can be more sufficient also to decrease cyber incidents. Procedures of cyber security were vital for information systems protection as it was provided the plans for security program generally and produced a stage to apply practices which is secure for the companies. Adnan (2017) justifies that In Malaysia, businesses are aware of cyber threats and data breaches. However, they are not doing any practical procedures to overcome it. The aim of the practices is to offer high quality managerial tracks and supports to secure the information along with agreeing business regulations and laws. Therefore, these implementations will lead into secure strategies of data asset.

C. Factors influencing Cyber security adoption

This part mentions the factors related to cyber security adoption from past studies including technological factors, organizational factors and individual factors. Despite that there is several studies discussed cyber security adoption. Majority of them disregarded the factors mentioned above. Therefore, it is plausible to review these studies for greater results. Bulgurcu et al. (2012) conducted study on cyber security policy compliance, the study discussed the rationality-based believes and cyber security awareness. It addressed the antecedents of employee's compliance with the cyber security policy of an organization. Particularly, the rationality based factors that lead employees to comply with cyber security policy with regard to secure the organization's cyber assets and critical infrastructure. Study found that an employee's intention to comply with cyber security policy is significantly influenced by attitude, normative beliefs, and self-efficacy to comply with cyber security policy. Gagnon et al. (2010) investigated Factors affecting the Adoption of ICT by Healthcare Professionals. Systematic literature of relevant databases explored studies regarding the interventions promoting Information and Communication Technology adoption by healthcare professionals. Analysis was conducted by using a particular grid. One hundred researches were included. The study found that the perception of system usefulness was significant factor besides perceived ease of use.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

D. Theoretical frame work

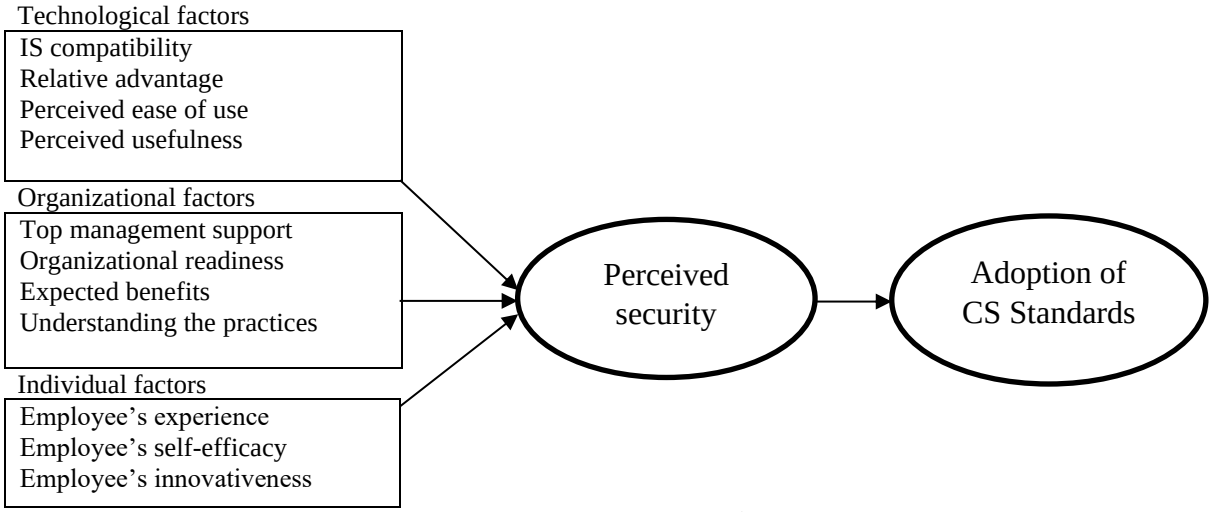

Fig.1. Theoretical framework

Past studies have investigated technological context in the context of cyber security implementation. However, the increasing security needs have caught researcher's attention to study other necessary contexts. (Soomro et al., 2016) while Qing Hu et al (2012) Studied factors affect employee behavior towards the adoption of cyber security policy; the findings have demonstrated that organizational factors including top management support in cyber security initiatives has significant effects on employees' behavior towards, subjective norm of, and perceived behavioral control over compliance with information security policies. In terms of individual factors studies found that experienced individuals are more likely to adopt and become familiar with information systems and computers. (Akman et al, 2016).

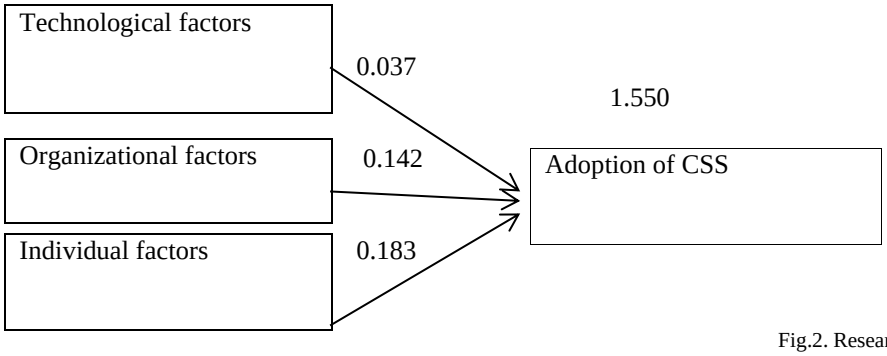

Fig.2. Research model

E. Perceived security

Perceived security can be traced back as the degree to which a user perceives that using IS will be free from any risk. Studies have shown that the feeling of security is largely determined by the users' feelings of control in any system [16]. Other studies that related to perceived security is rooted in the Technology Acceptance Model (TAM) which is an information systems theory that predicts how users respond to new technology. The premise is that external variables such as perceived security influence how and when users will use new technology [17]. In most recent studies, it has been utilized that user's adoption of cyber security is determined by several perceivable factors, such as the perceived usefulness, ease of use, which can make user's perceived security vary from the actual security level of an information system. The 'gap' between people's perceived security and the real security level of an information system can significantly affect their decisions and behavior. Lower perceived security can lead into rejection of cyber security standards, adoption. On the other hand, high perceived security may result users engage in insecure practices [18]. Thus perceives security considers as moderating variable in the adoption of cyber security standards in this study.

III. METHODOLOGY

Explanatory Research design has been chosen for this study since explanatory research is to examine a problem or situation to demonstrate the relationship between the variables. As this method consider one of the luckily methods to decide best way to deal with the research problems in order to achieve the research goals. Thus, in order to define the best research design, data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

collection method and the right information needed to accomplish this study, explanatory study was chosen. Quantitative approach is an experiment used to carry out the research. The scientific methods imply postulating hypotheses, doing quantitative experiments, and then either sustaining or rejecting hypothesis based on statistical analysis of the measured data. To be able to propose fruitful hypothesis, one must have a well-developed understanding of the research area. In addition, in order to gain statistically reliable results, the number of samples must be large enough for survey studies [19].

IV. RESULT ANALAYSIS

Coefficient results

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-2.737	1.550		-1.766	.079
	Technological factors	.037	.064	.082	2.104	.566
	Organizational factors	.142	.071	.287	0.955	.049
	Individual factors	.183	.030	.395	4.799	.000

Adoption of Cyber security standards= 0.37(technological factors) + 0.142(organizational factors) + 0.183 (individual factors) + 1.550

The table above shows coefficient of the variables. From the table the coefficient was used for technological factors was 0.037. Hence for every unit increase in these factors, there would be an increase in the adoption of CSS. The standardized beta value was 0.082 with t-value of 2.104. The p-value of this factor was significant. The unstandardized coefficient for organizational factors was 0.142 whereby for every unit increase in these factors there would be an increase in the adoption of CSS. The standardized beta value was 0.287 with t-value of 0.955. The p-value of this factor was significant. The unstandardized coefficient for individual factors was 0.183 whereby for every unit increase in these factors there would be an increase in the adoption of CSS. The standardized beta value was 0.395 with a t-value of 4.799. The p-value of this factor was significant as well. As recommendation, this study has focused on specific factors related to the technological factors, organizational factors and individual factors. However, other factors may also influence the adoption of CSS such as environmental factors and social engineering factors may bring insight from future research.

V. CONCLUSION

As information systems and cyberspace upsurge in complexity and volume, it is crucial to address cyber-threats and investigate cyber security vulnerabilities, to determine the best approaches and methods in coping with this issue in order to assist Malaysian public listed companies, since it contains large amount of technological and financial organization as it is subject to major cybercrimes to obtain a clear picture the key contributors to o combat the menace, avoiding sever data breaches and financial impacts.

VI. FUTRE RESRACH

This study has focused on specific factors related to the technological factors, organizational factors and individual factors. However, other factors may also influence the adoption of CSS such as environmental factors and social engineering factors may bring insight from future research.

ACKNOWLEDGEMENT

The author would like to thank Universiti Teknikal Malaysia Melaka (UTeM) for their
Support in obtaining the information for this work.

REFERENCES

[1] Carlos Roca et al. (2009). The importance of perceived trust, security and privacy in online trading systems. *Emarlad insight*, 99.
[2] Abbas et al. (2015). INFORMATION SECURITY MANAGEMENT FOR SMALL AND MEDIUM SIZE ENTERPRISES. *ISSN*, 2.
[3] Mat et al. (2019). Cybersecurity and Digital Economy in Malaysia: Trusted Law for Customer and Enterprise Protection. *International Journal of Innovative Technology and Exploring Engineering*, 2-3.
[4] Antonio et al. (2015). ADOPTION OF INFORMATION SECURITY MEASURES IN PUBLIC RESEARCH INSTITUTES. *Journal of Information Systems and Technology Management*, 290.
[5] Edward Hartono et al. (2014). Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation. *science diract*, 4.
[6] Huang et al. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *Science Direct*, 2-3.
[7] Hulsebosch et al. (2015). *inventory and classification of cyber security standards.* The Ministry of Security and Justice of the Kingdom of the Netherlands.
[8] Jones et al. (2010). Utilizing the Technology Acceptance Model to Assess the Employee Adoption of Information Systems Security Measures. *scholary commons*, 10.
[9] Karen et al. (2018). NIS website. *Emerald insight*, 10-11.
[10] Ling Li et al. (2019). Investigating the impact of cybersecurity policy awareness on employees cybersecurity behavior. *ELsevier*, 1-2.
[11] Mark Evans. (2016). Human Behaviour as an aspect of Cyber Security Assurance. *School of Computer Science and Informatics, De Montfort University, Leicester, UK*, 22.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 08, August-2020

[12] Muniandy. (2012). State of Cyber Security and the Factors Governing its Protection in Malaysia. *International Journal of Applied Science and Technology*, 7.
[13] Mohamed, M. (2015). *Cyber Security Standards Compliance: A Vital Measure to Critical Infrastructure Protection.* Malaysia: KBMG.
[14] Mark Saunders at el. (2016). *Research method for business students.* Harlow: pearson education.
[15] Safa et al. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*, 2-3.
[16] Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *ScienceDirect*, 430.
[17] Suhazimah, D. (2016). Social Factors Influencing the Information Security. *Association for Information Systems*, 9.
[18] Tofan, D. C. (2011). *Information Security Standards.* Bucharest: Academy of Economic Studies .
[19] Y. Arshad et al. (2014). Intelligent IT governance decision-making support framework for a developing country's public university. *Elsevier*, 131-132.