Cyber Security Threats Mitigation through Governance Framework and Cyber Security Market Solutions in Vietnam

Dr. Luong Cao Dong, Dai Nam University, Ha Noi, Viet Nam

Over the years, Vietnam has witnessed an increase in the number of internet users along with an increase in social media users who are always at risk of cyber threats in Vietnam. According to government statistics, internet users in Vietnam were witnessed to be around 64 million with active social media users to be around 62 million. In addition to this, mobile social media users reached approximately 58 million and the mobile subscription of Vietnam was witnessed to be around 143.3 million in the first quarter of 2019. Online payment transactions have increased which has increased the threat probability pertaining to user's data and systems. This has augmented the growth of the cyber security market in Vietnam. The specific objectives of this study are to examine the relationship of governance framework and oversight, market solutions - physical security, market solutions - logical security, market solutions - Internet of Things (IoT) and cyber security threats in Vietnam's businesses. The respondents are the businesses that have some sort of internet-enable computer system in Ho Chi Minh. The reason why this study only wanted to survey these people is because they are running the business themselves and they understand the cybersecurity threat factors that can contribute to the business success. Research outcomes shows that governance framework & oversight and market solutions - logical security have a significant positive relationship with cyber security threats mitigation among businesses in Ho Chi Minh, Vietnam. But, research findings showed that market solutions - physical security and market solutions – Internet of Thing (IoT) have no significant relationship with cyber security threats mitigation among businesses in Ho Chi Minh. Besides, from the R2 value of this study, the four exogenous constructs; namely (i) governance framework & oversight, (ii) market solutions - physical security, (iii) market solutions - logical security and (iv) market solutions - Internet of Things (IoTs) explained 38% of variations in the endogenous construct of cyber security threats mitigation in Vietnam's businesses. In addition, from the outcome of the blindfolding procedure, the endogenous variable of this study has a Q2 value of 0.270, which is described as medium because the value is far above 0.02.

Key words: *Governance Framework & Oversight, Market Solutions - Physical Security, Market Solutions - Logical Security, Market Solutions - Internet of Things, Mitigation of Cyber Security Threats, Vietnam's Businesses*

Introduction

Vietnam faces a lack of cyber security regulations to manage the cyberspace of the country. The first initiative in the cyber security market in Vietnam was in the year 2010 with a dedicated government roadmap (Glennon, 2012). Prior to this government roadmap, the initiatives in this domain were scattered and area focused. According to the industry statistics, around 61% of the personal computers in Vietnam are infected by malware and Vietnam is among the top countries with the highest rate worldwide of personal devices infected with viruses or malware. Therefore, a detailed and structured cyber security law is of utmost importance for Vietnam in the current scenario (Trân Dai, 2018).

Over the years, Vietnam has been observed to grow in terms of the amount of cybercrime and is on the edge of becoming a mid-tier cybercrime hub, opening opportunities for cyber security companies looking to tap into this market. Some of the major cybercrimes that the country witnessed during 2018 were crypto mining malware, ransom ware and others. Almost 60% of the network systems of agencies and enterprises were infected with crypto mining malware during the year 2018. As Vietnam has a price-sensitive economy, the domestic cyber security companies are grabbing this opportunity by providing low-cost security solutions. The majority of the domestic companies in Vietnam are only 10-12 years old and new domestic companies are expected to enter the market in the future. In addition to this, companies in the cyber security sector are expected to further push Vietnam into new areas of security solutions and services such as cloud security and Artificial Intelligence (AI) giving an optimistic outlook towards the market.

Out of the top five locations across the globe most at risk of infection, two are located in Southeast Asia: Vietnam and Indonesia. Both locations had a malware encounter rate of more than 45% in the second quarter of 2016, which is more than double the worldwide average of over 21% during the same period. Other top markets under malware threats include large developing markets and Southeast Asian countries – Mongolia, Pakistan, Nepal, Bangladesh, Cambodia, the Philippines, Thailand and India – each with encounter rates of more than 30 per cent.

To fulfill the objectives of the study, the general research question is "What are the determinants that have a significant impact on mitigating the cyber security threats in

Vietnam's businesses?" The specific research questions that need to be addressed are identified as follows:

1. Is there a significant relationship between governance framework & oversight and mitigation of cyber security threats in Vietnam's businesses?

2. Is there a significant relationship between market solutions - physical security and mitigation of cyber security threats in Vietnam's businesses?

3. Is there a significant relationship between market solutions - logical security and mitigation of cyber security threats in Vietnam's businesses?

4. Is there a significant relationship between market solutions - Internet of Things (IoTs) and mitigation of cyber security threats in Vietnam's businesses?

5. Among the three exogenous constructs, which will be the most significant construct that relates to mitigating the cyber security threats in Vietnam's businesses?

Theory & hypotheses

Governance framework & oversight

In a risk environment that is growing more perilous and costly, boards need to help steer their companies toward resilience and value by embedding strategic risk capabilities throughout the organisation (Trân Dai, 2018; Choras et al., 2015; Ayofe & Irwin, 2010). Today's corporate leaders navigate a complex environment that is changing at an ever-accelerating pace. Digital technology underlie much of the change (Jang-Jaccard & Nepal, 2013). Business models are being transformed by new waves of automation based on robotics and artificial intelligence (Wan & Alagar, 2014). Producers and consumers are making faster decisions, with preferences shifting under the influence of social media and trending news. New types of digital companies are exploiting the changes, disrupting traditional market leaders and business models. And as companies digitise more parts of their organisation, the danger of cyberattacks and breaches of all kinds grows (Trân Dai, 2018; Jang-Jaccard & Nepal, 2013). Beyond cyberspace, the risk environment is equally challenging. Regulation enjoys broad popular support in many sectors and regions; where it is tightening, it is putting stresses on profitability (Choras et al., 2015; Jang-Jaccard & Nepal, 2013). Climate change is affecting operations and consumers and regulators are also making demands for better business conduct in relation to the natural environment. Geopolitical uncertainties alter business conditions and challenge the footprints of multinationals. Corporate reputations are vulnerable to single events, as risks once thought to have a limited probability of occurrence are actually materialising (Trân Dai, 2018).

Market Solutions - Physical security

Physical security is often a second thought when it comes to information security. Since physical security has technical and administrative elements, it is often overlooked because most organisations focus on "technology-oriented security countermeasures" (Harris, 2013) to prevent hacking attacks. Hacking into network systems is not the only way that sensitive information can be stolen or used against an organisation. Physical security must be implemented correctly to prevent attackers from gaining physical access and taking what they want. All the firewalls, cryptography and other security measures would be useless if that were to occur. The challenges of implementing physical security are much more problematic now than in previous decades. Laptops, USB drives, tablets, flash drives and smartphones all have the ability to store sensitive data that can be lost or stolen. Organisations have the daunting task of trying to safeguard data, equipment, people, facilities, systems, and company assets. The company could face civil or criminal penalties for negligence for not using proper security controls. The objective of physical security is to safeguard personnel, information, equipment, IT infrastructure, facilities and all other company assets. The strategies used to protect the organisation's assets need to have a layered approach. It is harder for an attacker to reach their objective when multiple layers have to be bypassed to access a resource (Awan & Memon, 2016).

Market Solutions - Logical security

Today, security can mean either physical security, as in physical access control, or logical security (also known as cybersecurity), as in virus detection or unauthorised network access. The departments that manage the technology for these two types of security are usually entirely separate, and often do not even collaborate. With the proliferation of IP convergence on the network, this can have a dramatic impact on departments, as well as the safety and security of an organisation. This document describes the background and future trends of logical and physical security management; why the two departments need to collaborate, and why having a solid network foundation is critical to a solid security posture. A solid security policy starts at the top. Having a single, high-level individual or department responsible for a comprehensive security policy, whether actual or virtual, that covers both physical and logical security is paramount. Having executive sponsorship (such as CIO, CSO, and so on) as the governing body with cross-functional or cross-departmental teams for the requirements gathering and policy definition ensures that the various department-specific requirements are taken into account. Developing the security policy in silos hinders the ability to effectively deploy these policies.

Market Solutions - Internet of Things (IoTs)

With the rapid development of internet technology and communications technology, our lives are gradually led into an imaginary space of virtual worlds. People can chat, work, shop, keep pets and plants in the virtual world provided by the network (Giannikos, Korina, Fotiou, Marias, & Polyzos, 2013). However, human beings live in a real world; human activities cannot be fully implemented through the services in the imaginary space (Gang, Zeyong,& Jun, 2011). It is the limitation of imaginary space that restricts the development of the internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and the real-world on the same platform which is called the Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands in internet technology. It will bring huge changes to the future society and change our way of life and business models (Jiang & ShiWei, 2010).

Theoretical Framework

Derivied from the in-depth explanation in the section of background and problem statement, combined with the context of research in Vietnam, the author proposed three significant constructs that determine the level of cyber security threats in Vietnam's businesses, and they are: (1) Governance Framework & Oversight, (2) Market Solutions - Physical Security, (3) Market Solutions - Logical Security, and (4) Market Solutions - Internet of Things Threats (IoTs),

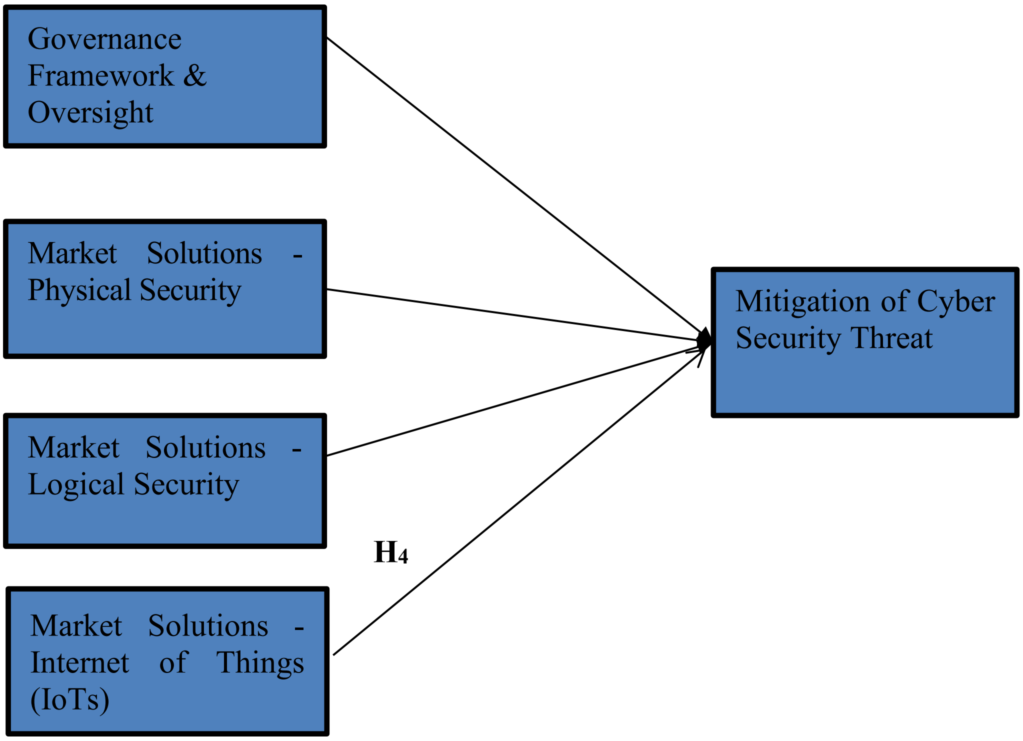
Governance Framework & Oversight
Market Solutions - Physical Security
Market Solutions - Logical Security
H4
Market Solutions - Internet of Things (IoTs)
Mitigation of Cyber Security Threat

Figure 1. *Research Framework*

Methodology

This study is a descriptive study because this study wants to establish the associations between governance framework & oversight, physical security, logical security and Internet of Things

(IoTs) that relate mitigating the cyber security threats in Vietnam's businesses. Finally, the hypotheses are confirmed. The data collection method is survey using a questionnaire with closed-ended questions. The results will provide numerical data that can be analysed statistically as the researcher looks for a correlation between governance framework & oversight, physical security, logical security and Internet of Things (IoTs) that relate to mitigating the cyber security threats in Vietnam's businesses. Furthermore, data gathered using questionnaires is usually more reliable (Zhang, Xiao, Ghaboosi, Zhang & Deng, 2012) as it enables the elimination or minimisation of judgment subjectivity (Oriyano, 2014).

Sampling and Data Collection Procedure

The devices used to collect data from the respondents are called data collection instruments. Data collection instruments can be in the form of tests, interviews, checklists or questionnaires (Seaman, 1998). In this study the data collection instrument is a questionnaire. According to the definition provided by Perera, Zaslavsky, Christen & Georgakopoulos (2013), the respondents are able to express their feelings, beliefs, attitudes and knowledge in the questionnaire. All the questionnaires in this study were designed in such a way that all the questions being asked are to collect information about cyber security threats in Vietnam's businesses. However, according to Burns & Grove (1993), there are also some weaknesses in validity and accuracy in the questionnaire. Some respondents might not answer according to their sincere opinion, some of them might only want to please the researcher and give a positive answer. Hence, some of the genuine and valuable information may be lost. Sometimes, lack of time in answering the questions or if the questions are too brief will also affect the quality of the questionnaire. In this study, the questionnaires were in English. There are two sections in the questionnaire. Section A of the questionnaires consisted of questions designed to obtain demographic data, for example age, gender, education level and previous experience. Section B aimed to determine the relationship between governance framework & oversight, physical security, logical security and Internet of Things (IoTs) that relate to mitigating the cyber security threats in Vietnam's businesses.

In terms of data analysis, this study will suggest Structural equal modelling for the development and testing of theories (Hair et al., 2012; Ringle et al., 2012). There are two parts in structural equation models estimation which are covariance-based SEM (CB-SEM) and variance-Based Partial Least Squares path modelling (PLS-SEM) (Hair et al., 2013; Rigdon, 2012). PLS-SEM is getting more and more popular in academic research (Hair et al., 2012, Ringle et al., 2012; Lee et al., 2011). Hair et al., (2014) has supported partial least squares structural equation modelling approach. This approach has gained popularity in accounting (Ringle, Sarstedt & Straub, 2012).), operations management (Ringle, Sarstedt & Straub, 2012).), marketing literature (Hair et al., (2013), strategic management (Hair et al., 2013), management information systems (Ringle et al., 2012) and organisational research (Hair et al., 2010). PLS is suitable for research in order to predict the relationship between two constructs. It is also useful in a complex model, research with a new theoretical model, a model which is not well-formed and a model with latent variables or structural paths (Chin & Newsted, 1999). In the present study, Smart PLS 3.0 path modelling is being used.

Results

In this study, the measurement model as depicted in Figure 2 was assessed as a reflective model using two stage and repeated items indicators approach. Thus, suggesting that at each stage, both individual item reliability and internal consistency reliability, as well as convergent and discriminant validity of the latent variables have to be established (Rasoolimanesh et al., 2016).

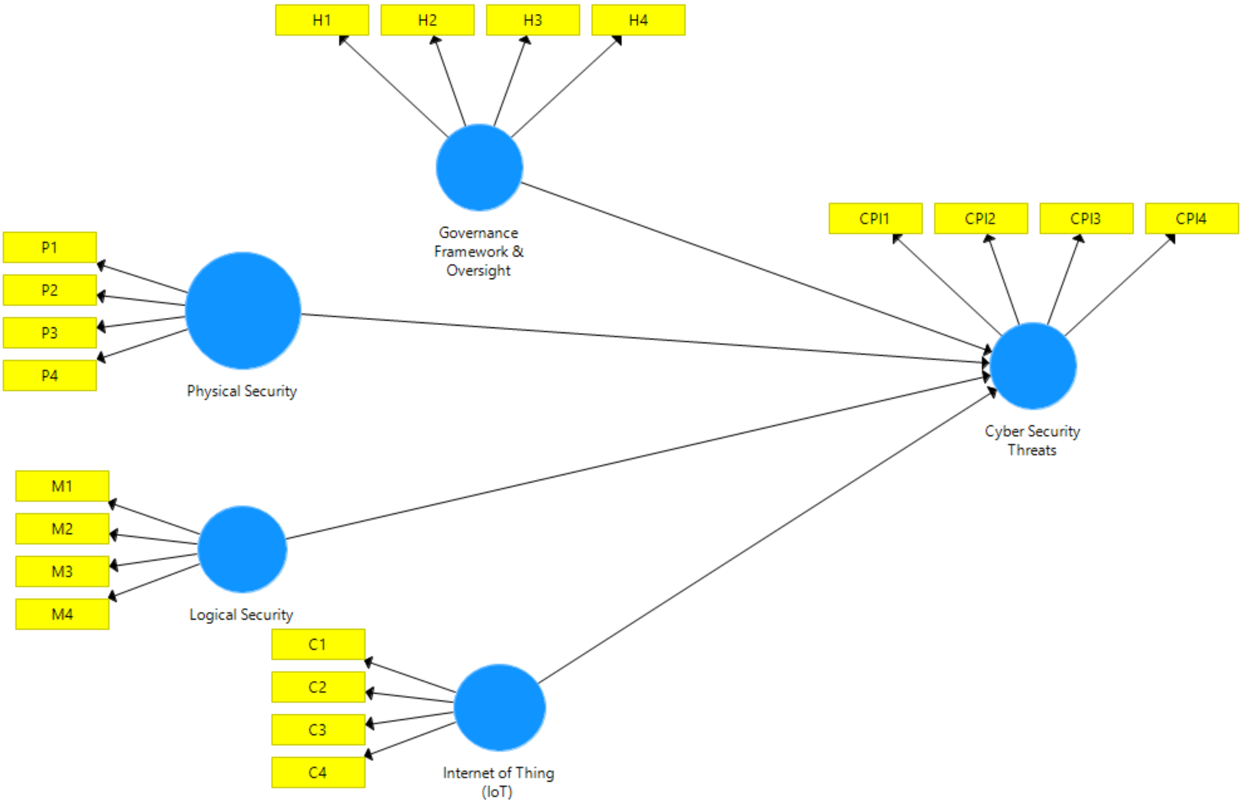

Figure 2. *Research Model*

According to Hair et al. (2014), the purpose of structural model is to determine the predictive abilities of exogenous variables on endogenous variable, through path coefficient, t-value and p-value, as well as R square, f square and predictive relevance. Thus, in this study, a Bootstrapping function of PLS-SEM which is also a non-parametric technique of determining the robustness of the statistical package was utilised using 108 observations and 5000 sub-samples, at 0.05 level of significance (Hair et al., 2014). Similarly, in this study, the R square, f square and predictive relevance were assessed using Bootstrapping and Blindfolding procedures of SmartPLS3.0. As depicted graphically in Figure 3 below, the study examined the direct relationship of governance framework & oversight, physical security, logical security & Internet of Things (IoTs) towards cyber security threats in Vietnam's businesses.

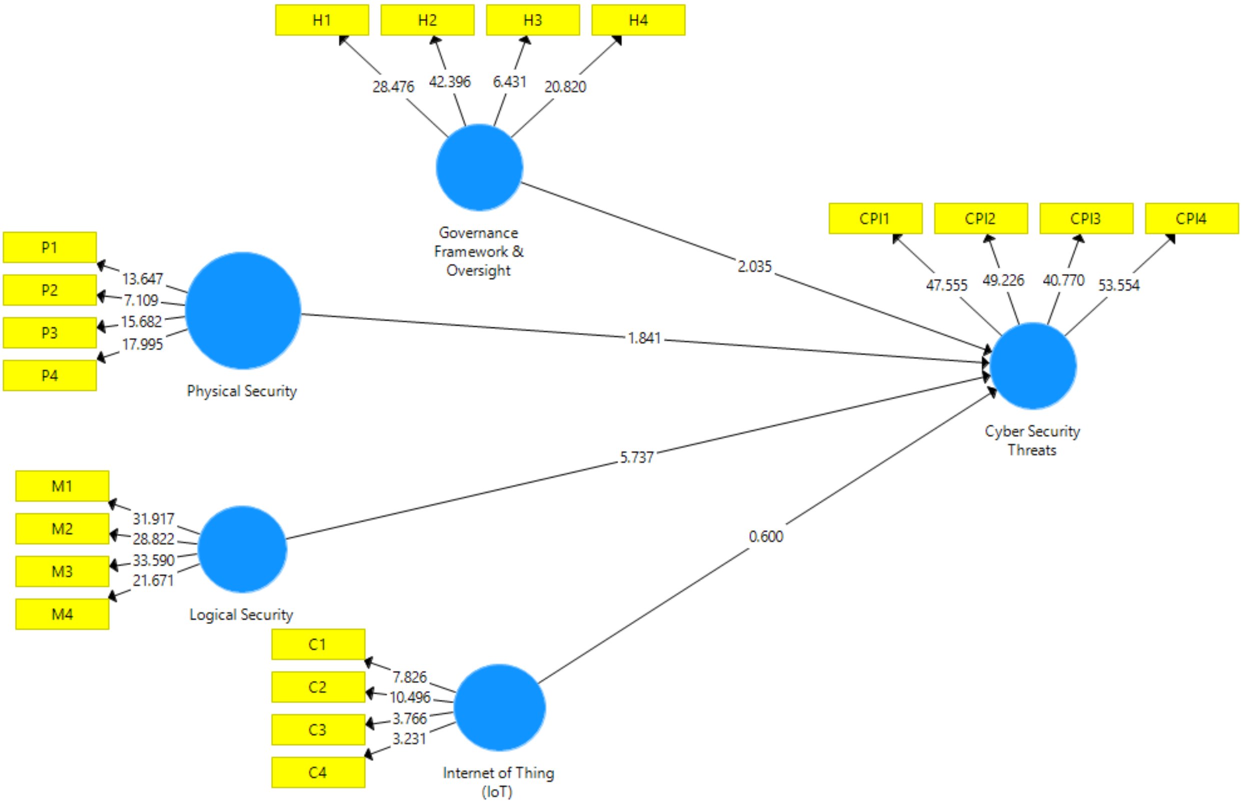

Figure 3. *Assessment of Structural Model*

Hypothesis 1 postulated that there is a significant relationship between Governance Framework & Oversight and Cyber Security Threats. The research outcome shows that Governance Framework & Oversight has a significant positive relationship with Cyber Security Threats among businesses in Ho Chi Minh, Vietnam ($\beta = 0.207$; $t = 2.035$; $p< 0.05$). Therefore, providing a statistical support for H1.

Hypothesis 2 postulated that there is a significant relationship between Logical Security and Cyber Security Threats. The research outcome shows Logical Security has a significant positive relationship with Cyber Security Threats among businesses in Ho Chi Minh, Vietnam ($\beta = 0.455$; $t = 5.737$; $p< 0.05$). Therefore, providing a statistical support for H2.

Hypothesis 3 postulated that there is a significant relationship between Physical Security and Cyber Security Threats. The research findings showed that Physical Security has no significant relationship with Cyber Security Threats among businesses in Ho Chi Minh, Vietnam ($\beta = 0.164$; $t = 1.841$; $p>0.05$). Therefore, H3 is not supported statistically.

Hypothesis 4 postulated that there is a significant relationship between Internet of Thing (IoT) and Cyber Security Threats. The research findings showed Internet of Thing (IoT) has no significant relationship with Cyber Security Threats among businesses in Ho Chi Minh, Vietnam (β = -0.034; t = 0.600; p>0.05). Therefore, H4 is not supported statistically.

Table 1. *Assessment of the Main Effects (Path Coefficient)*

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Governance Framework & Oversight -> Cyber Security Threats	**0.206**	**0.207**	**0.101**	**2.035**	**0.042**
Internet of Thing (IoT) -> Cyber Security Threats	**-0.052**	**-0.034**	**0.086**	**0.600**	**0.549**
Logical Security -> Cyber Security Threats	**0.455**	**0.466**	**0.079**	**5.737**	**0.000**
Physical Security -> Cyber Security Threats	**0.157**	**0.164**	**0.085**	**1.841**	**0.066**

Accordingly, the standardised beta coefficients of all the research constructs as depicted in Figure 4 below, it is empirically established that logical security has a highest positive beta value with cyber security threats among businesses in Ho Chi Minh, Vietnam (β = 0.455), followed by governance framework & oversight (β = 0.206) and finally physical security (β = 0.157). On the contrary, the internet of things (IoTs) hasa negative beta value (β = - 0.052), and the relationship with cyber security threats among businesses in Ho Chi Minh, Vietnam is not significant.

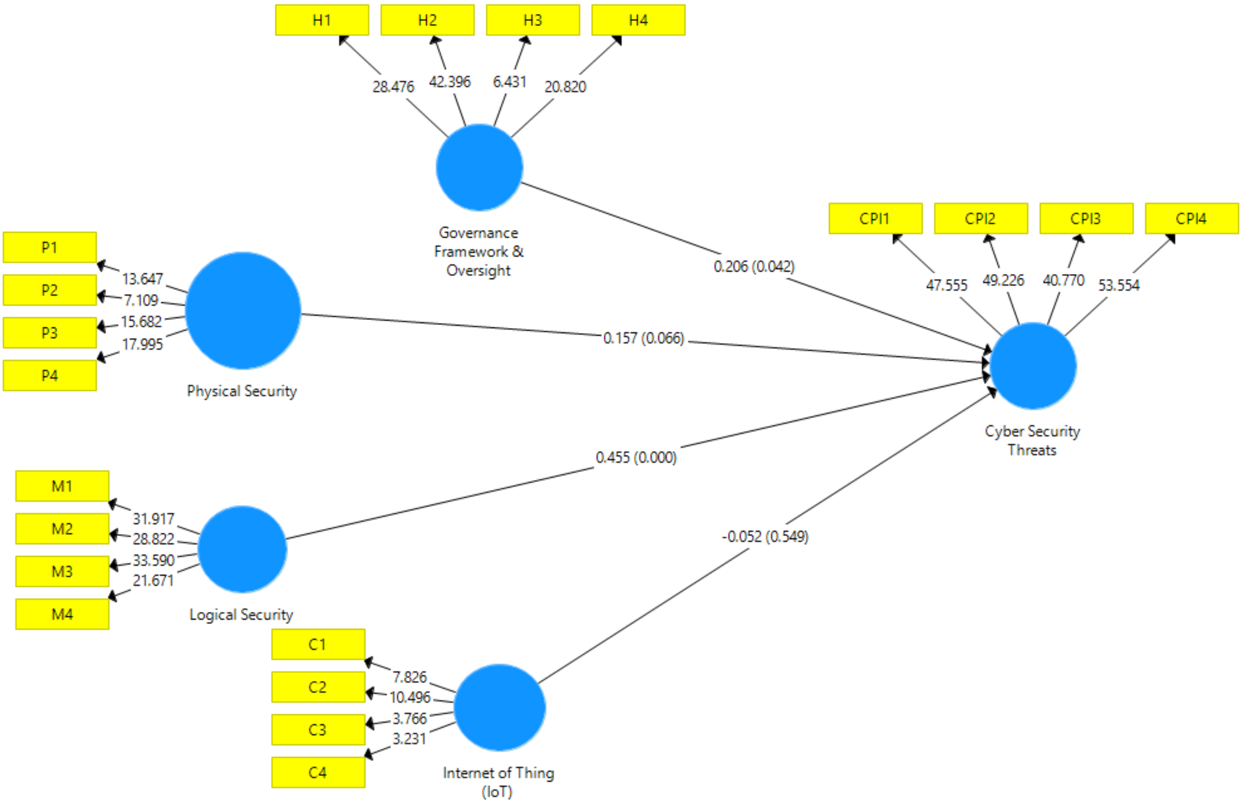

Figure 4. *Assessment of Structural Model with Beta Value*

According to Hair et al. (2012), the value of R square (R2) accounts for a variation explained by exogenous variables in the endogenous variable of a research model. Equally, Hair et al. (2010) argued that scholars have differed on the most suitable value of R2, though depending on the research setting. Consequently, a value of R2 above 0.10 is described as appropriate (Falk & Miller, 1992). On the other hand, Cohen (1988) described R2 values of 0.02, 0.13, and 0.26 as weak, moderate and substantial. In addition, Chin (1998) argued that R2 a value of 0.19 is still weak, while, the moderate value is 0.33 and substantial value is 0.67.

From the R2 value of this study, the four exogenous constructs; namely Governance Framework & Oversight, Physical Security, Logical Security & Internet of Things (IoTs) explained 38% of variations in endogenous construct of Cyber Security Threats in Vietnam's Businesses. Therefore, adopting the assessment criteria of Cohen (1988), the value of R2 in this study is substantial as showed in the Table 2 below:

Table 2
R Square

	R Square	**R Square Adjusted**
Cyber Security Threats	0.380	0.363

In this study, the predictive relevance of the model was assessed using Blindfolding technique of SmartPLS3.0. According to Sattler et al. (2010), predictive relevance is only acceptable on an endogenous construct in research with a reflective measurement model operationalisation. In addition, Hair et al. (2014) maintained that a predictive relevance of a model is determined through the value of Q2 which is calculated using omission distance that falls within the range of 5 and 7. Thus, in this study, omission distance of 7 was utilised in running the blindfolding technique. According to Hair et al. (2014), predictive relevance (Q2) can be small, medium and large. Based on the suggested assessment criteria, a value of 0.02 is described as small; while a value of 0.15 is described as medium; and lastly, a value of 0.35 is described as large. From the outcome of the blindfolding procedure, the endogenous variable of this study has a Q2 value of 0.270 as depicted in Table 3 and graphically in Figure 5. As a conclusion, the predictive relevance of the model is described as medium because the value is far above 0.02.

Table 3. *Construct Cross Validated Redundancy*

	SSO	SSE	Q^2 (=1-SSE/SSO)
Cyber Security Threats	600.000	438.256	0.270
Governance Framework & Oversight	600.000	600.000	
Internet of Thing (IoT)	600.000	600.000	
Logical Security	600.000	600.000	
Physical Security	600.000	600.000	

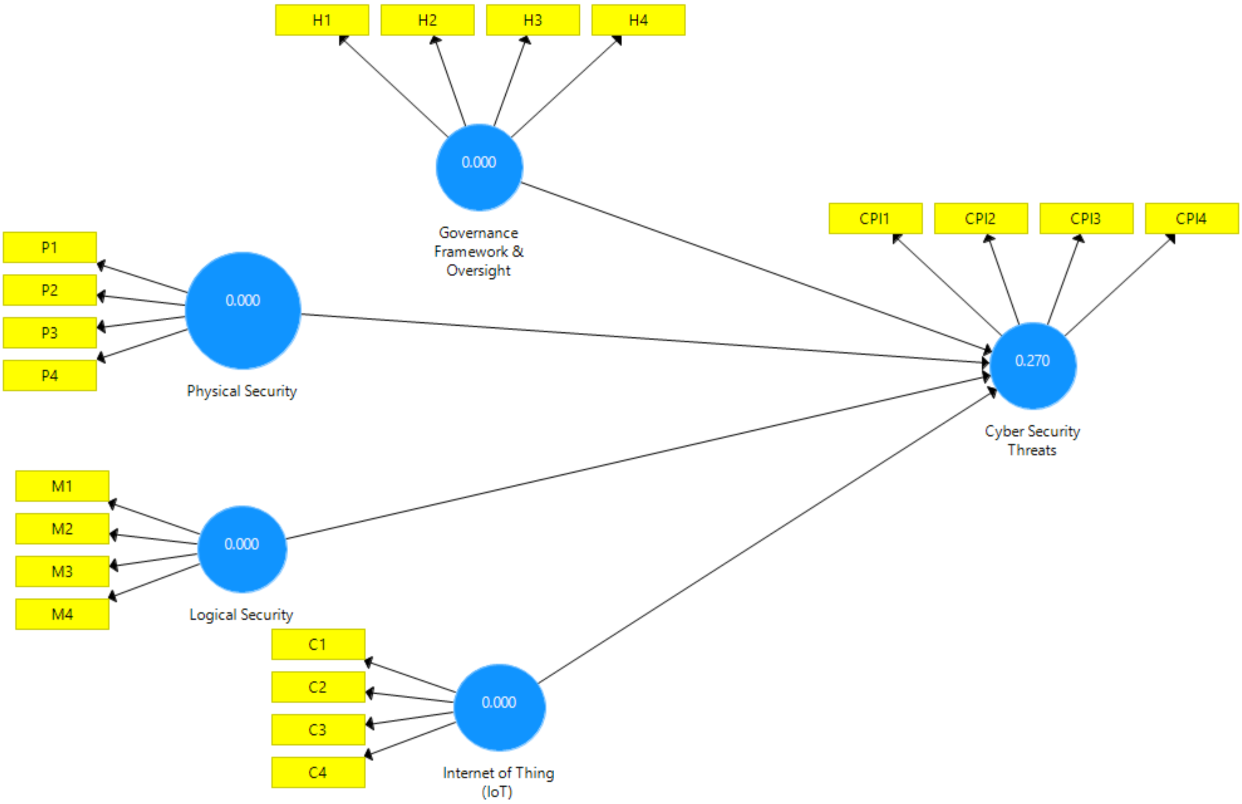

Figure 5. *Assessment of Predictive Relevancy*

Conclusion

People should implement a similar level of caution in the online world, as they do in the physical world. However, as non-physical threats seem less tangible and dangerous, generally it people less worried for their security. This study has shown how different cyber threats can disrupt human security and the following part will conclude the discussion. The review of the literature affirmed that cyber space is borderless and accessible for all – creating issues like too much anonymity, difficulty of attribution and lack of cyber hygiene among the general public. The debate in the academic literature about cyber incidents is state centric and the concerns are war-related. There is not much information about individual threats or how cyber-attacks are connected to people's security in the online sphere. However, human security in cyber space should be as important as it is in the physical world.

However, using the human security concept as a basis for research and analysis definitely has its pros and cons. As the concept had never been used in relation to the cyber sphere, it was complicated at first to find the associated pieces; only indirect connections between the two exist, which had to be identified and interpreted by the author. Accordingly, human security is quite a vague concept for the basis of an analysis, as there is no one certain definition or framework. On the other hand, the lack of defined structure gave the author the chance to look at the concept from her own perspective and facilitated an original approach to cybercrime. Furthermore, human security is a good way to look at the topic, as securing people's actions online should be necessary, and this concept gives the right extent of flexibility and authority to do that.

REFERENCES

Awan, J., & Memon, S. (2016). Threats of cyber security and challenges for Pakistan. In International Conference on Cyber Warfare and Security (p. 425). Academic Conferences International Limited.

Ayofe A. N. & Irwin, B. (2010). Cyber security: Challenges and the way forward,'' Comput. Sci. Telecommun., 29(6), 56–69.

Choras, M., et al., (2015). Comprehensive approach to increase cyber security and resilience, in Proc. 10th Int. Conf. Availability, Rel. Secur. (ARES), 686–692. doi: 10.1109/ARES.2015.30

Chouhan, R. (2014). Cybercrimes: Evolution, detection and future challenges. IUP J. Inf. Technol., 10(1), 48–55.

Federation of European Risk Management Associations (FERMA) (2017). At the junction of corporate governance and cybersecurity – 2017.

Gang, G., Zeyong,L., & J. Jun, J (2011). Internet of Things Security Analysis. 2011 International Conference on Internet Technology and Applications (iTAP), 1-4.

Giannikos, M. Korina, K, Fotiou, Marias, G & Polyzos, G. C. (2013). Towards secure and context-aware information lookup for the Internet of Things. In Computing, Networking and Communications (ICNC,) Proceedings of IEEE , 632-636.

Glennon, M.J. (2012). State-level cybersecurity. Policy Rev.,171,85–102.

Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2014). A primer on partial least squares structural equation modeling (PLS-SEM): Sage Publications.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate data analysis (7thed.). New Jersey: Prentice-Hall.

Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The use of partial least squares structural equation modeling in strategic management research: a review of past practices and recommendations for future applications. Long Range Planning, 45(5), 320-340.

Harris, S. (2013). Access Control. In CISSP Exam Guide (6th ed., pp. 97, 98, 157- 277). USA McGraw- Hill.

Harris, S. (2013). Information Security Governance and Risk Management. In CISSP Exam Guide (6th ed., pp. 21-141). USA McGraw-Hill.

Harris, S. (2013). Physical and Environmental Security. In CISSP Exam Guide (6th ed., pp. 427-502). USA McGraw-Hill.

Henseler, J., & Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. Structural Equation Modeling, 17(1), 82-109.

Henseler, J., & Fassott, G. (2010). Testing moderating effects in PLS path models: An illustration of available procedures Handbook of partial least squares, 713-735, Springer.

Henseler, J., & Sarstedt, M. (2013). Goodness-of-fit indices for partial least squares path modeling. Computational Statistics, 28(2), 565-580.

Henseler, J., Wilson, B., Götz, O., & Hautvast, C. (2007). Investigating the moderating role of fit on sports sponsorship and brand equity. International Journal of Sports Marketing and Sponsorship, 8(4), 34-42.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993.

Jiang,D & ShiWei, C (2010). A Study of Information Security for M2M of IoT. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 576-579.

National Cyber Security Institute (2016). Accessed online: http://www.nationalcybersecurityinstitute.org/general-public- interests/top-2016-cyber- threats-for-small-businesses http://www.cbsnews.com/news/percentage- of-companies- that-report- systems-hacked/ (Accessed on 12 October 2019).

Oriyano, S. (2014). Physical Security. In Cehv8: Certified Ethical Hacker Version 8 Study Guide (pp. 393-409). Indianapolis, IN USA: Wiley.

Podsakoff, P. M., MacKenzie, S. B., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. Annual review of psychology, 63, 539-569.

Rigdon, E. E. (2012). Rethinking partial least squares path modeling: in praise of simple methods. Long Range Planning, 45(5), 341-358.

Rigdon, E. E., Schumacker, R. E., & Wothke, W. (1998). A comparative review interaction and nonlinear modelling.

Ringle, C. M., Sarstedt, M., & Straub, D. (2012). A critical look at the use of PLS SEM in MIS Quarterly. MIS Quarterly (MISQ), 36(1).

Ringle, C. M., Sarstedt, M., & Straub, D. W. (2012). Editor's comments: a critical look at the use of PLS- SEM in MIS quarterly. MIS quarterly, 36(1), iii-xiv.
State of Play, Progress and Future Prospects. Governance Systems for Cybersecurity, 86- 97.

Trân Dai, C. (2018). Cybersecurity Governance Framework in Vietnam:

Vietnam Computer Emergency Response Team (2018). Vietnam Cyber Security Industry Outlook to 2023. [Access Online: www.vncert.gov.vn]

Wan,K & Alagar,V. (2014). Context-aware security solutions for cyber physical systems. Mobile Netw. Appl., 19(2), 212–226.

Zhang, Y. Xiao, Y., Ghaboosi, K., Zhang,,J. & Deng,H. (2012). A survey of cybercrimes. Secur. Commun. Netw., 5(4), 422–437.