



Cybercrimes in the Banking Sector: Case Study of Vietnam

Le Thanh Tam¹, Nguyen Minh Chau², Pham Ngoc Mai², Ngo Ha Phuong², Vu Khanh Huyen Tran², Phi Hong Hanh³

¹ School of Banking and Finance, National Economics University, Hanoi, 10000, Vietnam

² School of Advanced Educational Program, National Economics University, Hanoi, 10000, Vietnam

³ Aviva Vietnam Life Insurance Company Limited, Hanoi, 10000, Vietnam

Corresponding author: *Le Thanh Tam*. Email: tamlt@neu.edu.vn

Received 18 May 2020;

Accepted 23 May 2020;

Published 31 May 2020;

ABSTRACT

The technological revolution 4.0 brings great opportunities, but also cybercrimes to economic sectors, especially to banks. Using secondary data and primary data from survey of 305 bank clients, the main findings of this paper are: (i) there are several types of cybercrimes in the banking sector; (ii) Vietnam is one of the top countries worldwide having hackers and being attacked by hackers, especially the banking sector. Three most common attacks are skimming, hacking and phishing. Number of cybercrime attacks in Vietnam are increasing rapidly over years; (iii) Vietnamese customers are very vulnerable to cybercrime in banking, as more than 58% seem to hear about cybercrimes, and how banks provide services to let them know about their transactions. However, more than 50% do not have any deep knowledge or any measures for preventing cybercrime; (iii) Customers believe in banks, but do not think that banks can deal with cybercrime issues well. They still feel traditional transactions are more secure than e-transactions; (iv) the reasons for high cybercrimes come from commercial banks (low management and human capacity), supporting environment (inadequate), legal framework (not yet strong and strict enough on cybercrimes), and clients (low level of financial literacy). Therefore, several solutions should be carried out, from all stakeholders, for improving the cyber security in Vietnamese banks.

Keywords: *Banking, Cybercrime, Phishing, Skimming, Online, Technological Revolution*

1. INTRODUCTION

The technological revolution 4.0 with the application of advanced technology has transformed the operation of many industries and is step-by-step striving for sustainable growth in the economy (Lenon et al, 2019; Mohammed Bazzoun, 2019). It is well predicted that this will create new opportunities for companies and business to improve on their operation, management and competitiveness, as connections and productivity has increased significantly (Pereira & Romero, 2017; Cotteleer & Sniderman, 2017). Together with great opportunities, technological revolution also makes cybercrime more difficult to control, more complicated and increased in occurrence (Lennon, 2017). The victims vary from individual technology users to corporates and even the states, while the crime's characteristics make it difficult to investigate (Martellozzo & Jane, 2017). In the banking sector – one of the most dynamic economic sectors and directly related to financing issues of all stakeholders in society, the cybercrime issues are much more problematic. Criminals in banking are often skillful, can utilize a broad range of Information and Communications Technology (ICT) applications to penetrate, manipulate and attack bank accounts, information systems or more, and operate internationally, which makes cybercrime an extremely alarming threat to every country (Smith, 2015).

Vietnam is a developing country that has achieved steady economic growth recently, partly thanks to its advancement of technology. However, this also means that the country began to rely heavily on technology, especially its banking sector (Le & Pham, 2018; Malik & Islam, 2019), and therefore become exposed more to the cybercrime threats. Whereas domestically there are few researches on such significant topic, the available information and studies are limited and incomprehensive. Additionally, these studies could hardly cover the latest updates of the problem, and some might not be able to capture the scale of cybercrime from within Vietnam. This is the research gap for the authors to do the research on "Cybercrimes in the banking sector: Case study of Vietnam".

2. LITERATURE REVIEW

2.1. What is cybercrime in the banking sector?

"Cybercrime" or "Online crimes" are used to call "High-tech crimes". According to Yewkes & Yar (2011), there are no consistent definitions for "Cybercrime". Thomas & Loader (2010) stated that cybercrimes include activities using computers that may be illegal or identified as illegal by some organizations, and these activities can be done via the global electronic network. In addition, Halder & Jaishankar (2009) argues that cybercrime is "an

offense with intentional harm to the victim's reputation, physically or mentally, or creating loss to victims indirectly or directly, using modern methods such as the Internet (via chat rooms, e-mails, online notice boards or guild groups) and electricity mobile phone (via SMS or MMS)". In other words, "Cybercrime," or "high-tech crime," is the term for criminal offenses that occur with the Information Communications Technology (ICT) platform used with illegal purposes (Hunton, 2009; Kraemer-Mbula et al., 2013). In Vietnam, the cybercrime is "crime committed by intentionally using knowledge, skills, tools, information technology at a high level to unlawfully affect information. numbers stored, processed and transmitted in computer systems, infringing upon the order of information security, damaging the interests of the State, the legitimate rights and interests of organizations and individuals " (GoV, 2014). Therefore, cybercrime in banking is the crimes with high-tech relating to the banking sector or clients for illegal purposes. Today's cybercriminals are as savvy and professional as the businesses they attack. This maturity calls for a new perspective on the multifaceted nature of cyber threats and accompanying frauds.

2.2. What are types of cybercrime in banking?

Aggarwal G. (2015) classified cybercrime into 13 types: Hacking (accessing into a person's computer without his knowledge to achieve personal, confidential information), Theft (violating and breaking copyrights to download data, which is known as pirated data), Identity theft (stealing information about bank account, credit card, debit card numbers and other confidential data to make transaction under the victim's name), Defamation (hacking email accounts and sending negative emails to destroy the dignity of the victim), Malicious software (using software to gain access to a system then steal confidential information and/or damage the hardware or software of the system), Cyber stalking (bombarding the victim with online messages), E-mail harassment (harassing the victim by sending him letters, attachments), Spoofing (acting as the victim to illegally have access to his data), Fraud (stealing the victim's money in his bank account by making transactions from his account), Virus (loading on a computer with a program that cause damage to the system), Trojan horse (convincing the victim to download a code that harms the system), Phishing (sending false emails to gain confidential information then use it against the victim), and Grooming (creating a relationship with children for sexual exploitation).

According to Wall (2001), cybercrime criminals can be divided into four groups: Cyber-trespass (infringing upon someone's property and/or cause damages such as intrusion, humiliating and creating virus), Cyber-deception and thefts (stealing money, property, or infringing intellectual property), Cyber-pornography (violating the rules of obscenity and human dignity), and Cyber-violence (causing psychologically or instigating damage to a person. This violates the human body protection). This way of classification divides the criminals into three groups of cybercrime criminals: "Criminals against properties", "Criminals against morality", and "Criminals against the person".

In Criminal Code of Vietnam, two types of cybercrime criminals are stated: (i) Criminals using computers, digital devices, computer networks, telecommunication networks to cause damage to the security, integrity and availability of computer systems; and (ii) Criminals using computers, digital devices, computer networks, telecommunication networks as tools and means for committing crimes (National Assembly, 2017).

From literature review, the types of cybercrime in banking are summarized as followed:

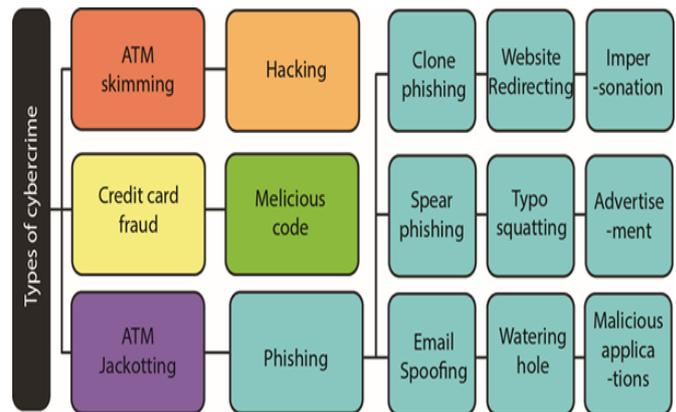


Figure 1. Types of cybercrimes in banking sector

Source: Authors' compilation from literature review

3. MATERIALS AND METHODS

The research was conducted with the process summarized as in Figure 2 below.

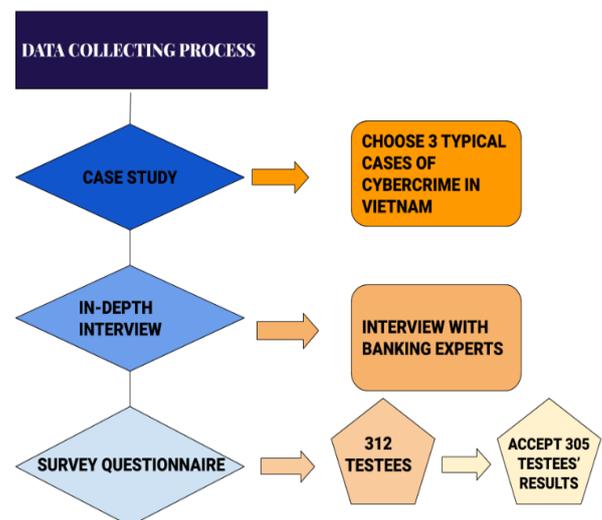


Figure 2. The research process

Source: Author's compilation

In order to get insights into the situation of cybercrime in the Vietnam banking sector, both qualitative and quantitative methods are employed, using secondary and primary data. As secondary data of cybercrime in banking sector topic is very scattered and not systematic, primary data from in-depth interviews and structured questionnaires with 312 individuals, of which only 305 can be used. The development of questionnaires followed the process of developing according to literature, pilot and revised, and implemented in the period of October 2018-Jan 2019.

4. RESULTS

4.1. Overall cybercrime situations of Vietnam banking sector

Vietnam is ranked number 8th in terms of countries from which the highest percentage of Global Denial of Service Attacks (DDoS) originated. Among top countries worldwide, there were only the appearance of Vietnam and China as developing countries.

Table 1. List of countries from which highest percentage of Global DDoS originated

Country	China	USA	UK	France	Korea	Singapore	Japan	Vietnam	Germany
%	29.56	21.59	16.17	8.72	4.06	3.93	3.81	3.76	3.49

Source: Goud (2019)

Vietnam experienced a total number of 6219 cyber-attacks by July 2019, increasing 104% compared to 2018, with 3824 deface, 2155 phishing and 240 malwares. In addition, nearly 100,000 computers were infected with a malicious virus each day (Doan, 2019; VNS, 2019).

4.2. Cybercrime in banking sector via customers’ views

In this section, the interview results of 305 customers were analyzed to understand their views on cybercrimes in the banking sector in Vietnam.

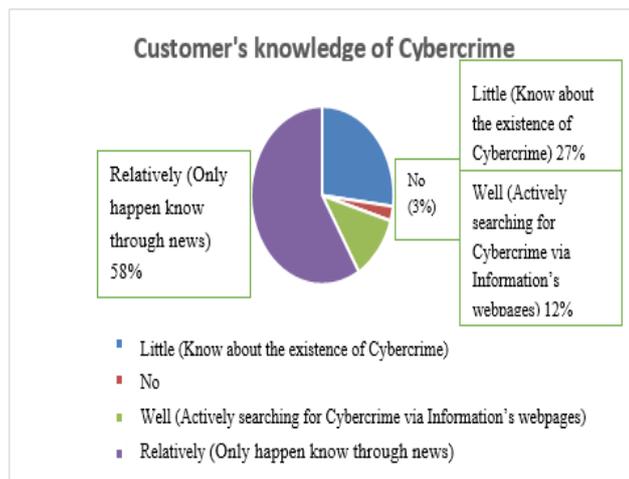


Figure 3. Customer opinions on the safety and convenience when using Bank's high-tech services

Source: Authors’ compilation from primary data

About 58% of the customers relatively knew about cybercrime through the mass media, and 12% of them actively looked for information by themselves. A quarter of the participants had only heard of cybercrime and there were 8 people who had never heard of it. This is an alarming situation when cybercrime has been developing very fast in recent years and the awareness of customers play a vital part in preventing it. The two kinds of securities offered by banks which are known most by respondents (more than 50%) are One-time Password (OTP) and SMS Banking. Firewall and chips rank second with slightly more than 20% of people knowing about them. On the bottom of the list is the new technology called 3D Secure due to its novelty and popularity to online-shoppers only. Apart from listed types of securities, RSA and Key-pass OTP has also been mentioned by some correspondents. However, the results show that about nearly 10% bank account users do not know any of the security methods, indicating that these users are very vulnerable to cybercrime issues.

In terms of customers’ knowledge of cybercrime prevention, with the increase in cybercrime attacks, 76.72% of people being asked on the matter prove that they are aware that banks are at stake of being cyber-attacked. However, nearly half of the sample responded that they do not know how to deal with cybercrime if they are involved in attacks and 66% of the sample demand more information from banks about cyber-attacks and solutions that customers can apply.

When talking about the safety they feel when using banking services, most respondents (up to 90%) feel quite safe, given not having been attacked by cybercrime when using the banking services provided. Up to 135 people out of 305 are not clear about the bank's security policies and procedures. When compared to the results of the easy-to-understand and easy-to-follow levels of security terms, a positive correlation is found: 131 people feel that they cannot be evaluated and up to 14% think they have difficulty in this matter. Most respondents conclude that traditional transactions are safer. Automated Teller Machine (ATM) service has the number of people finding its security unreliable up to 69.51%.

For direct assessment of banks, more than 80% of customers expect the bank to take better measures in both preventing and dealing with cybercrimes. In addition, it shows that banks have been very active in taking measures to prevent risks and promptly informing customers about changes with concurrence of 79.34% and 57.77% respectively. However, customers do not think that the security system is regularly updated with more than 46% of respondents giving neutral ratings when it comes to this issue.

5. DISCUSSIONS

In this section, the detailed analysis bases on the results above will be conducted. Therefore, the in-depth comprehensiveness towards the issue will be clarified and work as the premises for the later potential suggestions and recommendations.

5.1. Overview of cybercrimes in Vietnam’s banking sector

Not only in the world but in Vietnam context let alone, Cybercrime contains various types along the distinguished level of complexity. From the previous section, the current stage of Cybercrime as well as the awareness of Cybercrime among part of Vietnamese residents were staged in terms of statistics and figures.

Among cybercrimes in the banking sector, three most common attacks are skimming, hacking and phishing. First, skimming - one of the most popular methods that cybercrime applies to take over bank’s customers’ properties (Tam & Thao, 2018). The Ministry of Public Security’s C50 Division has arrested dozens of suspects on charges of skimming in ATM and bank card-related crimes between 2015 and 2017, with damages ranging from hundreds to billions of VND (Van Anh, 2018). Victims of credit card skimming are often unaware of the theft until they notice unauthorized charges to their accounts or have their cards unexpectedly declined (N.A., 2019).

Second, hacking – to steal customer’s properties and personal information through the bank's online services. Vietnam has 64 million internet users, representing 66% of the population. The figure gives Vietnam the 12th-highest number of users in the world and ranks it sixth among 35 countries and territories in Asia (Hootsuite, 2019). In terms of bank hacking, Vietnam was in the top 10 countries worldwide, with 52.07% of internet users attacked by malicious programs, and 23.7 percent of users in the country were attacked by web-borne threats (Lan, 2016; N.A, 2016).

Third, phishing or “fake attack” - an activity of constructing the fraud system to steal sensitive information such as log-in name, password or credit card information. Not surprisingly, Vietnam has recorded a lot of phishing attacks in many different forms, such as: clone phishing, malicious applications, advertisement, impersonation, watering hole, typosquatting, website redirect, email spoofing, spear phishing. Phishing appears as a trustworthy entity or can be accessed easily through shopping online web pages or even through famous online platforms such as Amazon, Paypal, Gmail and online banking. Phishing is often performed through email, often in the form of one-click mail or links to access or redirect into the fraud websites. Current phishing cases are focusing more on the bank’s customers or online payment services (Thinh, 2018; N.A, 2018).

5.2. Cybercrimes in Vietnamese customers’ view

• Customers’ assessment on the level of handling cyber-attacks

Considering the ways banks tackle the cyber-attacks, the majority of customers remain neutral on judging this issue. This can be explained by the fact that cyber-criminals attack individual accounts rather than the banking system, thus the attacks are not known by other account users. Also, the information on these cases are not communicated to customers so that banks can defend their positions and reputation.

The lack of information can be witnessed by further looking into how bank users judge the tackling of cybercrime from the view of: time to tackle, solution to customers, involvement of police and sentences for cyber-criminals. About half of all the people being asked feel satisfied with banks seeking help from police to deal with cyber-attacks. However, the period of time to find the criminals is still inadequate, as well as the judgments and solutions to the situations. The results of the cases all raised the same problems. This is what the banks should consider to improve. Moreover, when being asked about the measures that the bank should apply to avoid cybercrime, the majority could not give specific answers to the question. So it can be seen that awareness as well as the level of initiative of customers on this issue is not high, and needs to be improved.

• Safety concern

The majority of customers, though favoring the benefits of high-tech services, still do not fully believe in the security level of banks because they are not fully educated in the security system. Therefore, customers have the expectation that the bank will take actions to secure their assets.

• Overall assessment of customers’ viewpoints on cybercrimes in banking sector

From primary data results, it can be concluded that Vietnamese banking customers have a certain understanding and different opinions on cybercrime. Most of the respondents have a limited range of age and income, which caused some difficulties in accessing the index of customers who own large amounts of assets, yet the research could have a refreshing way to consider the young and dynamic customer framework. Another remarkable point is that the respondents are customers of many different banks, especially of the Big 4 banks in Vietnam (BIDV, Vietinbank, Agribank and Vietcombank), which provides the study with an overview of the current situation of banks.

In recent years, when information technology has been quickly developed and high-technological services are applied by banks, the users feeling satisfied with the utilities that they bring

could be considered common sense in daily life. Customers always want the bank to develop equivalent services, while also ensuring the security of their assets. Customers have almost never been attacked by cybercriminals, but it does not affect their perception that this is a problem which needs to be addressed. The frequency of encounters among the surrounding people encountered cybercrime attack gets higher, whereby more and more cases were mentioned making customers worried and hope for more appropriate and advanced security policies from banks. Due to the complexity of cybercrime cases, customers could not have enough information to fairly assess the situation. They did not fully trust the banks’ ability to handle these situations. However, they show their faith to banks when banks actively work with the authorities.

5.3. Reasons for high cybercrimes potential in Vietnam’s banking sector

The fact of high cybercrime potential in Vietnam has originated from many aspects.

First, from commercial banks: (i) Low management level, and the cybercrime precautions of banks have not been considered thoroughly. Many of the banks’ security procedures are not strict enough. The development of services such as e-banking or mobile banking is creating a lot of space for criminal development. (ii) The lack of highly qualified human resources in information technology is also one reason that makes them bear cybercrime problems. (iii) The types of high-tech security used in the banks still provide cybercrime many potential chances to attack. Although banks have realized the importance of information security and have applied measures to keep the system secured, browsers and applications that the bank has been using are not highly effective. Some applications require human manipulation, which can hardly help banks to catch up with the instant pace of cybercrime’s development; (iv) investment requirements for security and Information Technology (IT) application of banks are more and more expensive, which not all banks can update or pay frequently.

Second, from supporting environments such as technology infrastructure, training, information sharing. Although the bank’s security systems are being upgraded, they still have a lot of loopholes. The loopholes in the high-tech system recorded in the cases in Vietnam mainly come from the link between the network operator and the bank, especially in the process of sending the confirmation / verification message of OTP code / bank account activation code. Once they have the victim’s phone number, it is not difficult for cybercrimes to seek the authentication code from their victim’s account. This is also a base condition for cybercrime to attack and cause significant financial and reputation damage to the bank. More specifically, these loopholes appear as a result of the gap, in which cyber crimes’ activities have become more and more sophisticated while the security system of banks is still weak and not timely updated to combat this metamorphosis.

Third, from policy makers: (i) the legal framework shows many deficiencies because it has not updated fully the acts of disguise of cybercrime. All the regulations were enacted in 2015, and up to now, many cases of cybercrime discovered with more complex aims and methods; (ii) the number of sanctions of cybercrime punishment is very limited. The regulation only clarifies the two behaviors of fraudulent access and theft of property, and illegally publicizes bank account information; (iii) the violations have not been clarified. Specifically, to the crime of illegally publicizing information of bank accounts, the law only

stipulates that the general violations will be suspended from working from 1 to 5 years. This is a big limitation because it does not show what a general violation is, making it difficult to apply in practice; (iv) the penalties are not strict enough. Vietnam's highest penalty is only 12 years in prison. Not only that, the distinguished provisions for the use of high-tech to steal property only have a maximum sentence of 5 to 10 years in prison depending on the nature of the crime and whether the act is a recidivism or not.

Fourth, from individuals and other stakeholders: The biggest cause for criminals to be able to attack the bank's high-tech system despite the modern security is applied is by the carelessness and lack of knowledge of the customers. Customers sometimes still not understand thoroughly the service processes provided and they hardly spend much time to learn all about them. In addition, there are individuals who use the service carelessly and without vigilance, resulting in the leak of information for illegal purposes.

6. CONCLUSIONS

Currently, Vietnam has founded the Cyber Security and Cybercrime Prevention Department (A05) under the Ministry of Public Security of Vietnam. This Department will be in charge of assuring the Cyber Security and proposing measures to prevent, detect and handle Cybercrime, especially in Banking sector. The Government requests Vietnam banking sector to strengthen remuneration mechanisms, attracting more high-tech units to meet the needs of the Industrial Revolution 4.0 with clear orientation to 2025 and vision 2030 (GoV, 2018, Minh, 2018). In order to support banks to apply high technologies in operation, the SBV will continue to improve the legal framework for the new technological products; create an environment that supports Fintech companies to creatively find solutions to cybercrime problems.

To enhance Banking security, lower and prevent the increase in Cybercrime, these measures below should be taken into consideration:

For commercial banks: (i) Enhance the quality of Banking security software; (ii) Active in surveilling security performance to detect the possibility of technology gaps and cybercrime activities in time; (iii) Boost the completion of assuring card payment safety, strictly surveil and give permission to run business to those card payment units that meet the appointed criteria of safety; (iv) Provide fully and in time information about Cybercrime, such as: Current trend, tricks; Along with any change happens to occur in Banks; (v) Complete the conversion of Magnetic card to Chip card; (vi) cooperate with fintechs to minimize the costs and increase the efficiencies/innovations in cybercrime prevention.

For policy makers: (i) Update the 2015 version of Legal framework terms about Cybercrime to be more appropriate for the current stage of Cybercrime; (ii) Adjust more rules and regulations to handle Cybercrime in Banking sector; (iii) Concretize each violation under the terms related to Cybercrime; (iv) Increase the severity of penalty for Cybercrime activity, in which the sentence penalty can go up to 25-30 years; Classify each type of Cybercrime based on the level of damage to determine the crime and the appropriate penalty; (v) For minor crimes, there should be deterrent rules and remedies along with supervision to avoid recidivism.

For supporters in the ecosystem (technology infrastructure, training, information sharing): (i) Improve the quality of the high technologies being used currently in Banking systems. (ii) Improve core banking, Artificial Intelligence (AI) system; applying

blockchain in information management and to replace the old transaction instruments.

For Customers: (i) Improve the knowledge and skills for fully understand all of the services provided by banks; (ii) Create safe and strong password that meet the criteria of each party providing paying services; (iii) Update regularly security browsers for current used applications; (iv) Understand the distinctiveness of all Cybercrime types; (v) Keep alert on risks of bank cards (stealing information through ATMs, stealing information through old cards, unused cards).

ACKNOWLEDGEMENTS

This research is funded by National Economics University, Hanoi, Vietnam.

We are very grateful to the participants, interviewees of this study for all the time and effort they have put into the suggestions and advice that helped us complete this study. We also want to express our deep gratitude towards our family and dear fellows who have helped us along the implementation of this study from the very beginning. Lastly, we would like to send our greatest appreciation to the National Economics University for creating a great environment for us to accomplish the study.

STATEMENT OF COMPETING INTERESTS

We - The authors declare that there is no competing interests regarding the publication of this paper.

REFERENCES

- [1] Lennon, O., T., Tomlin, B., "Industry 4.0: Opportunities and Challenges for Operations Management", Tuck School of Business Working Paper No. 3365733, March, 2019
- [2] [Online] Available: <http://dx.doi.org/10.2139/ssrn.3365733> [Accessed Oct. 5, 2019]
- [3] Bazzoun, M., "The Digital Economy", International Journal of Social Science and Economic Invention, 116, September 2019
- [4] Pereira, A. C., and Romero F., "A review of the meanings and the implications of the Industry 4.0 concept", Procedia Manufacturing 13, 1206–14, 2017.
- [5] Cotteleer M. and Sniderman B., "Forces of change: Industry 4.0", Deloitte Insight.
- [6] [Online] Available: <https://www2.deloitte.com/insights/us/en/focus/industry-4-0/overview.html>, 2017. [Accessed Oct. 5, 2019]
- [7] Lennon Y.C.C., "Cybercrime and Cyber Security in ASEAN", Chapter 10, Book of Comparative Criminology in Asia, 135-148, Monash University (Australia), 2017.
- [8] Martellozzo, E. and Jane, E.A. (eds), "Cybercrimes and its victims", Routledge, London and New York, 2017
- [9] Smith, G. S., "Management models for international cybercrime", Journal of Financial Crime, 22 (1), 104-125, 2015.
- [10] Le T.T. and Pham T.T.T., "High-tech crimes for Vietnam banking industry in the context of industrial revolution 4.0: Current

situation and some policy recommendations”, *Journal of Science and Banking Training*, 192, 1-9, 2018.

[11] Malik, M. and Islam, U. “Cybercrime: an emerging threat to the banking sector of Pakistan”, *Journal of Financial Crime*, 26(1), 50-60.

[12] [Online] Available: <https://doi.org/10.1108/JFC-11-2017-0118>, 2019 [Accessed Oct. 15, 2019]

[13] Yewkes, Y. and Yar, M., “Handbook of internet crime”, Routledge, London and New York, 2011.

[14] Thomas, D. and Loader, B., “Introduction – cybercrime: law enforcement, security and surveillance in the information age”, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, London, 2010.

[15] Halder, D., Karuppanan, J., “Cyber Socializing and Victimization of Women”, *The Journal on Victimization*, 12(3), 5-26, *Human Rights and Gender*, September 2009.

[16] [Online] Available: <https://ssrn.com/abstract=1561774>. [Accessed Oct. 9, 2019].

[17] Hunton, P., “The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model”, *Computer Law & Security Review*, 25(6), 528-535, 2009.

[18] Kraemer-Mbula, E., Tang, P. and Rush, H., “The cybercrime ecosystem: Online innovation in the shadows?”, *Technological Forecasting and Social Change*, 80(3), 541-555, 2013.

[19] Government of Vietnam, “Government Decree No. 25/2014/NĐ-CP dated April 07, 2014 on crime prevention and other law violations using high technology”, 2014.

[20] Aggarwal, G., “General awareness on cybercrime”, *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(8). 204-206. 2015.

[21] Wall, D. S., “Crime and the Internet: Cybercrimes and Cyberfears”, Routledge, 1st ed., 2001.

[22] National Assembly, “Law No. 12/2017/QH14 dated June 20, 2017 to amend some articles of the Criminal Code No. 100/2015/QH13”, 2017.

[23] Goud, N., “List of countries which are most vulnerable to Cyber Attacks”, *Cybersecurity Insiders*.

[24] [Online] Available: <https://www.cybersecurity-insiders.com/list-of-countries-which-are-most-vulnerable-to-cyber-attacks/> [Accessed Oct. 5, 2019]

[25] Doan, E. Z., “Number of cyber attacks in Vietnam in 2018, by type”, Statista.

[26] [Online] Available: <https://www.statista.com/statistics/1030774/vietnam-number-of-cyber-attacks-by-type/> [Accessed Oct. 5, 2019]

[27] VNS, “Vietnam records more than 6,200 cyber attacks in seven months”, *Vietnam News*, August, 2019

[28] [Online] Available: <http://vietnamnews.vn/society/523433/viet-nam-records-more-than-6200-cyber-attacks-in-seven-months.html#1AdgPyZ1cTWmKS1b.99> [Accessed Oct. 1, 2019].

[29] Tam, L. T., Pham Thi Thu Thao. (2018), High-tech crimes for Vietnam's banking industry in the context of industrial revolution 4.0: Current situation and some policy recommendations, *Journal of Science and Banking Training*, Vol. 192, Banking Academy

[30] Van Anh, “Recent Agribank thefts may have featured skimming devices”, *Vietnam Investment Review*, April, 2018.

[31] [Online] Available: <https://www.vir.com.vn/recent-agribank-thefts-may-have-featured-skimming-devices-58759.html> [Accessed Oct. 1, 2019].

[32] N.A, “Vietnam Banks take steps to fight card fraud”, *Vietnamnet Global*, May, 2019.

[33] [Online] Available: <https://vietnamnet.vn/en/business/vn-banks-take-steps-to-fight-card-fraud-528299.html> [Accessed Oct. 9, 2019].

[34] Hootsuite, “Digital 2019 Vietnam”, February 2019.

[35] [Online] Available: <https://www.slideshare.net/DataReportal/digital-2019-vietnam-january-2019-v01>. [Accessed Oct. 9, 2019].

[36] Lan, T.T, “Cyber fraud unearths potential loophole at Vietnamese bank's security system”, *VN Express*, August, 2016.

[37] [Online] Available: <https://e.vnexpress.net/news/news/cyber-fraud-unearths-potential-loophole-at-vietnamese-bank-s-security-system-3452158.html> [Accessed Oct. 5, 2019]

[38] N.A., “Vietnam among 10 countries most exposed to hacking risk”, *VnExpress*, November, 2016

[39] [Online] Available: <https://e.vnexpress.net/news/news/vietnam-among-10-countries-most-exposed-to-hacking-risk-report-warns-3505435.html> [Accessed Oct. 9, 2019].

[40] Thinh, C., “VNCERT warns of malware attacks on banks”, *The Saigon Times*, July, 2018.

[41] [Online] Available: <https://english.thesaigontimes.vn/61478/vncert-warns-of-malware-attacks-on-banks.html> [Accessed Oct. 9, 2019].

[42] N.A., “Customers falling for fake bank clerk phishing scam”, *Vietnam Investment Review*, August, 2018.

[43] [Online] Available: <https://english.vov.vn/economy/customers-falling-for-fake-bank-clerk-phishing-scam-402216.vov> [Accessed Oct. 11, 2019].