Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 6, July, 2021: 9365 - 9372

Research Article

Model Of Cyber Crime Investigation In Thailand: Fraudulent Cases

Essarapong Tiprapakool [a*], Dr. Sunee Kanyajit [b], Dr. Patchara Sinloyma [c], Dr. Apasiri Suwannanon [d], Montree Yimyam [e]

[a*] Faculty of Social Sciences and Humanities, Mahidol University, Thailand
[b] Associate Professor, Faculty of Social Sciences and Humanities, Mahidol University, Thailand
[c] Professor Police Major General, Faculty of Forensic Science, Royal Police Cadet Academy, Thailand
[d] Assistant Professor, Graduate School, Rajabhat Suan Dusit University, Thailand
[e] Police Major General, Royal Thai Police, Thailand

: [a]artafapsrpca@gmail.com, [b]suneekanyajit@gmail.com, [c]sinloyma@gmail.com, [d]apadrphd@gmail.com

Abstract

This research aimed to study problems of cybercrime investigation of law enforcement officers in order to suggest model management of cybercrime investigation in fraudulent cases. This research was qualitative research by conducting in-depth interviews with 30 key informants. Research instruments were in-depth interviews and data analysis by content analysis. The research revealed that problems of cybercrime investigation were caused by law enforcement agencies and officers. The agencies that were in charge of suppression of cybercrime lacked forces, technologies, and maintenances and had no preparedness when compared to workloads. Besides, there were problems of distributing duties within the agency and also a lack of cooperation from technology service providers. The model management of cybercrime investigation in fraudulent cases comprised inquiring and explaining information before receiving a report, investigating officers gathering information, inquiring of victims about information supporting the investigation, recovering social media account, identifying criminals, and gathering acquired information to submit a request for information from service providers.

Keywords: Investigation Model, Inquiry, Cybercrime, Fraud, Social Media

1. Introduction

Currently, information technology systems are constantly developing. These inevitably become part of our life when using this information technology to develop and enhance work performance or help our everyday lives easy and satisfying human's needs in every part. Consequently, the human culture of living has changed that people resort to using the internet to facilitate ways of living (Saruang, 2019). Furthermore, mobile banking also helps financial transactions to be more convenient and brings about behavioral changes in producers and consumers. In 2017, it was found that there were 30 million accounts of mobile banking users in Thailand, but in 2018, there were 41 million accounts (Wayupap, 2019). Technological advancement is used by criminals to commit crimes. Especially, online fraud is committed by using communication via the internet against a person,

computer data, or computer system in order to cause errors to the working system or display. As a result, a person who commits such an offense gains benefits in one's property unlawfully (Saruang, 2019). _

The current statistics of online fraud threats are found growing. The statistics from the Thailand Computer Emergency Response Team: ThaiCERT stated that in 2018, threats of online fraud ranked second after the use of algorithms of computer data. The threat of using the algorithm of computer data was 43.9% followed by online fraud with 36.9%. Also, in 2019, threats of online fraud ranked first with 40.2% (Thailand Computer Emergency Response Team, 2020). The aforementioned problems require a tool to prevent and suppress crime that is an investigation so that the case will be substantiated to ask the court to impose penalties on offenders. The researcher, therefore, is interested in studying the model management of cybercrime investigation of the Technology Crime Suppression Division by focusing on cybercrime investigation in order to apply findings to determine strategies and projects for developing cybercrime investigation of Thailand.

2. Literature review

The study of model management of cybercrime investigation in Thailand: fraudulent cases reviewed criminological concepts and theories. The principle of the deterrence theories is that criminals are afraid of law and law enforcement or being arrested if they commit crimes. Therefore, criminals will do no crime if there are stringent law enforcement, laws with severe enough penalties, or the possibilities to commit crimes are slight. The theory emphasizes the significance of the "possibility" to commit crimes. These theories can be concluded that effective crime prevention requires measures or approaches to reduce the possibilities of criminals committing crimes because general criminals commit crimes without considering the benefits which they will obtain after committing crimes. (Khantee, 2015).

Another theory is the Differential Associations Theory that has been developed by Edwin Sutherland. Sutherland stated that criminals learn criminal behaviors and they are favorable to such behaviors. Learning elements are divided into 2 elements: 1) element of content includes special techniques to commit crimes, adequate inspiration, stimulus, and having a way of thinking following such behaviors. 2) Element of learning refers to learning processes that may occur to those who are both close and not close to each other, but they observe and imitate each other. In addition, there are other important elements such as learning frequency, learning period, and concentration. Sutherland extremely focuses on the concentration that has the greatest influence on learning behavior (Khantee, 2015). According to the aforementioned theory, it can be concluded that cybercrime contributes to learning. This is a new entry into Thailand that is accepted and violent on the part of damage and rapidity of damaging. Besides, cybercrime affects the minds of the victims. Learning crime methods and imitating crimes are based on the Social Learning Theory and the Differential Associations Theory (Khantee, 2015).

Moreover, there are 3 general principles for maintaining the reliability of evidence including the authentication of evidence, the chain of custody, and evidence validation. Firstly, authentication of evidence, which is a collection of evidence and those who are in charge of collecting evidence at the scene are crucial. Secondly, chain of custody is that maintaining evidence when changing hands. Lastly, evidence validation, which is general evidence can be easily noticed from its external conditions whether the change occurs, and can be photographed to verify the validation. However, for electronic evidence, what is important is data that is stored in electronic devices. The question often arises that how to be able to verify the validation that data stored in such devices will remain intact and not be modified later. Even though there is no intention to modify data of electronic evidence, being unaware by opening data or opening it with a computer used to verify without knowledge can extremely change the file of electronic evidence.

Crime investigation, the tendency of new cybercrimes, and cybercrime prevention and control are to be able to find the problem in cybercrime investigation in order to acquire evidence to arrest criminals. If the investigation sector can improve the ability in investigating and gathering evidence that is the essence to electronic evidence such as processes of gathering electronic, techniques and methods to prevent crime scene, examination of sites and online tracking in cybercrime investigation, basic principles of electronic evidence separation with explanation, refined processes of cybercrime investigation, creation of simulations of cybercrime investigation and gathering of evidence (Wu et al., 2019; Braga, Flynn, Kelling, & Cole, 2011). These elements of the investigation are essential for more effective cybercrime investigation (Pisarić, 2015; Sun, Shih & Hwang, 2015).

Furthermore, the previous research revealed that the justice process in cybercrime cases is delayed since officers lack knowledge and expertise, and there are inadequate supporting officers. Additionally, it is due to the difficulty of collecting evidence that needs to seek from the outsource and private sectors (Dechsakul & Trimek, 2019 Leukfeldt,Veenstra & Stol, 2013; Police Executive Research Forum, 2018 , Holt & Bossler, 2012). The majority of agencies also lack cooperation between public and private agencies related to cybercrime

prevention. Consequently, the prevention of cybercrime cannot be carried out in the same direction and it is inconsistent, resulting in duplicate operations (Siripongwattana & Pakdeenarong, 2015). Moreover, in cybercrime suppression, there are limitations on budgets and human resources and a lack of specialists with specific knowledge. The budget is insufficient to purchase up-to-date tools or protective equipment (Harkin, Whelan & Chang, 2018; Holt & Bossler, 2012; Sutriyanitipakdee, Techagaisiyavanit and Borwornnuntakul, n.d.).

Oonjai (2020) revealed that the quality of work life of police regarding adequate and fair compensation was at a low level. Chen and Burstein (2006) studied factors affecting the success of knowledge management and found that a successful organization requires knowledge management. There are three factors of implementing knowledge management strategy, including people, policies, and technologies. Each factor differently affects the success of knowledge management strategy. This can be concluded that knowledge management refers to collecting, systemizing, storing, and accessing information to create the knowledge that is related to knowledge sharing. Besides, there are 4 steps of behaviors within an organization regarding knowledge management culture including knowledge creation, knowledge processing, knowledge dissemination, and the use of knowledge (Borwornchai, 2020). Furthermore, the research revealed that police cooperation on cybercrime has been developed by additional training through Nordic Computer Forensics Investigators (NCFI)'s programs and Nordplus in order to enhance the efficiency of cybercrime investigation and to meet the demands of training of police officers (Leppänen & Kankaanranta, 2017).

3. Research Methodology

This research was qualitative research. The researcher conducted the collection of data on one's own. There were three key informant groups: 10 police officers from the Technology Crime Suppression Division were purposively selected from those who had at least 3 years of work experience in cybercrime investigation with at least 50 cases, 10 police officers from local police stations under the Metropolitan Police Bureau and Provincial Police Region were purposively selected from police officers who had at least 3 years of work experience in cybercrime investigation with at least 50 cases, and 10 officers from the Department of Special Investigation were purposively selected from those who had at least 3 years of work experience in cybercrime with at least 5 cases.

The researcher conducted individual interviews with an in-depth interview which is two-way communication by taking notes and recording audio during interviews with key informants from various groups in order to collect detailed information to cover the method of cybercrime investigation. Each interview took about 90 minutes. For data triangulation, the researcher implemented the following steps: 1) to interview police officers/officers of DSI with the same question from the same informant several times to verify the reliability of data that acquired data is consistent every time and 2) there was data verification from key informants of other sources who were cooperative with the researcher and had work experience in cybercrime cases, including police officers from the Technology Crime Suppression Division, local police officers from Metropolitan Police Bureau or Provincial Police Region, and officers from Department of Special Investigation. For the data acquired from individual interviews with an in-depth interview regarding cybercrime investigation in fraudulent cases, the researcher processed the data and analyzed qualitative data by using content analysis to determine the topic/category and conceptual pattern that is the essence of this research.

4. research results

According to interviews, requesting information from service providers was extremely problematic. Service providers often late to submit information supporting the investigation. They often have reasons that literally are excuses; for example, claiming that the information requester is not a computer officer. However, according to the law of Thailand, for a request for information and gathering of evidence of police officers to prove the guilt or innocence of the accused, police officers and law enforcement officers can submit a request according to authorities prescribed in the Penal Code, and do not need to be the officer under the Computer Crime Act B.E.2550 (2007) (and Amendment 2017). Consequently, it becomes more difficult to gather evidence. Moreover, if such service providers are located in foreign countries such as transferring money via western union or defrauding via Facebook, Instagram, and VK that their companies are located overseas, it is extremely difficult to request cooperation.

Another problem is preparedness of equipment, both hardware, and software used in officers' performances is that they are quite outdated. Even if the agency has tried to provide such equipment, there is an issue with the official regulations. Conversely, while law enforcement officers are attached by regulations of purchasing equipment like hardware and software, criminals can easily afford modern technological equipment. Some of the aforesaid equipment can be provided but cannot be used to their full capacity due to a small number of officers who are specialized to use such equipment and programs.. For various office equipment and programs

supporting the investigation, officers must pay with their own money, and these are also inadequate to meet the demand and cannot be used in time. Officers must pay for these services in advance or even programs used in the investigation that officers must use their personal money to purchase them.

The imbalance between forces and workloads is also a problem. There are crimes in every society inevitably. Conversely, despite the popularity of social media, the number of officers performing duties does not increase. Due to a large number of workloads with a small number of officers, some crimes are not truly solved and victims do not receive mitigation. Consequently, criminals become bolder and commit more crimes. Furthermore, cybercrime investigation requires specific knowledge regardless of patterns, but what has happened is that there are too few specialized officers and they do not pay attention to learn or improve themselves. There are certain crime patterns that the investigating officers do not pay much attention to because they consider that such a crime may not happen to them. But in fact, crime can occur in different patterns at any time. When a criminal considers that there is a gap in society, crime certainly occurs. In addition, considering the provision of such training programs, nowadays, various agencies have more interest to provide training programs. Nevertheless, since officers themselves pay no attention to learn, learning is not extended and the agency eventually becomes ineffective.

Most police officers performing duties at the local police stations are clearly assigned duties that there is no cooperation within the agency. As a result, the inquiry sector must be the only sector to confront and solve problems of the cases reported by people without enough support from the investigation sector. Furthermore, because of complicated and detailed duties in each case, former cases have been not finished yet, but officers need to solve new cases that are coming up. Consequently, officers are unable to get down into the details of every case. Those who have the intention of doing are probably discouraged. The researcher is able to analyze and synthesize problems of cybercrime investigation of the Technology Crime Suppression Division as shown in Figure 1

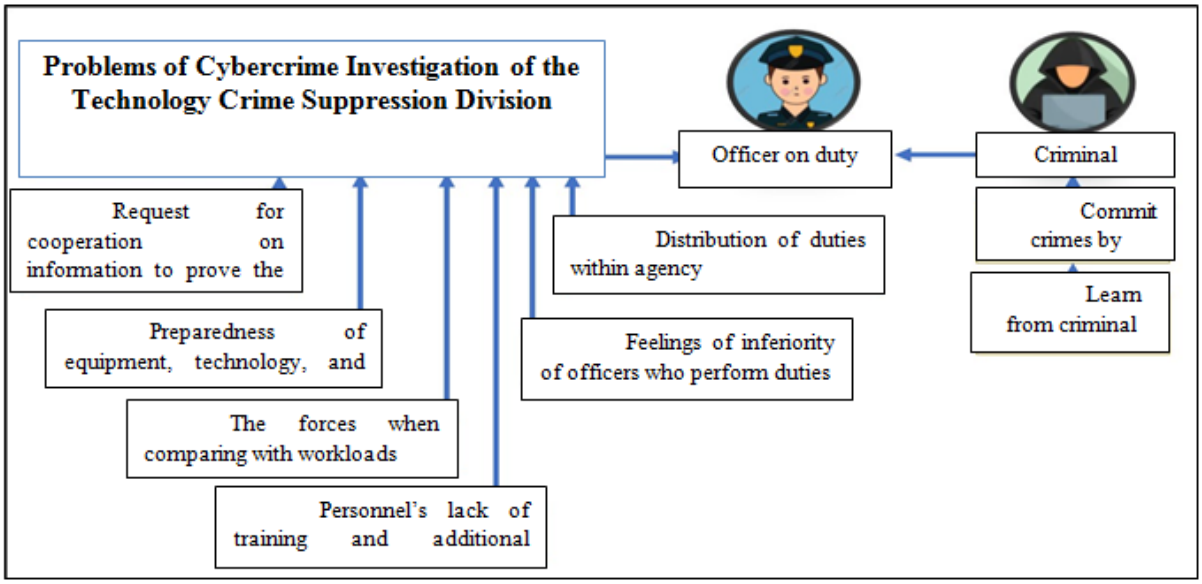

Figure 1 Problems of Cybercrime Investigation in Fraudulent Cases

According to interviews with key informants who perform duties of cybercrime investigation until become specialized, there are steps as follows:

Before filing a report, there are 2 parts, which are 1) police officers' operations when victims come to file reports and complaints; firstly, police officers will ask victims that where did such an offense occurs for the valid legal proceedings under the Criminal Procedure Code, and for convenience of victims who come to file reports and complaints. After the locality of the scene having been known, police officers start examining the evidence whether such an act committed by a criminal against a victim is a fraudulent offense.

Investigating officers gathering evidence, mostly, the pattern commonly found is service or what a victim needs; for example, deceiving by using love and claiming that a criminal has strong feelings for a victim. This sort of thing is called a romance scam. Another second pattern found by officers is Email scam. This is the way criminals impersonate as trading partners. Inquiring of victims about information to support the investigation, the way criminals can successfully commit offenses is partly because victims themselves believe that the accused can bring them the agreed advantages. For this reason, if criminals say or convince of anything, victims

will be obedient to follow what criminals said, or even other frauds. Basically, victims will tell officers that they still do not believe that they were defrauded. Therefore, victims sometimes do not give all of the information to officers who receive reports because they still withhold the information in case that the accused can do what they have claimed.

Recovering social media accounts, the investigation of fraudulent cases becomes quite more difficult nowadays since criminals use fake social media accounts for communicating. Therefore, when victims come to police officers, on the part of TCSD, investigating officers will immediately conduct an inquiry since the evidence are fresh. Consequently, officers can search names and surnames from the civil registration and conduct an inquiry immediately. Officers sometimes use information from public news such as searching from websites (Google) or public news in order to gather those evidence to support further investigation. Identifying (Criminals). scientific evidence is regarded as essential since it is evidence used to prove the guilt of the accused and cannot be changed. Accordingly, the evidence must be scientifically and promptly collected without contamination. Previously, when victims coming to file reports, they usually take a screen capture on their phone that such evidence is suspected and can also be suspicious in other justice processes.

Gathering acquired information to inquire of service providers is necessary to immediately integrate information to identify criminals. It is because the information on a computer can be stored only 90 days, so if it exceeds 90 days, service providers cannot hold such information due to legal restrictions. Furthermore, the samples also agreed that cybercrime investigation in fraudulent cases is an important duty that requires competent officers. Consequently, samples agreed with knowledge management of cyber investigation toward fraud in order to effectively carry out the investigation. In knowledge management of cyber investigation toward fraud, the samples deemed that in addition to having to be additionally trained, officers must be hopeful for the success of the cases for clearly-defined goals and being able to see successful solutions of the cases. Moreover, officers require full energy and also love in their work. Officers also need to try to disseminate knowledge and regenerate new investigators for maintaining knowledge and developing coordination in neighbor agencies that are used in the investigation.

5. Discussion and Conclusion

The research revealed that the problem of cybercrime investigation is the lack of cooperation from service providers for requesting information to prove the guilt of the accused because cybercrime requires scientific evidence to prove the guilt of the accused. Cybercrime case is different from general cases in that cybercrime cases require systems of service providers (internet service providers). These service providers have the storage of internet users' data at each moment. That is, there is a storage of data, namely the IP address in each access to the internet. Such IP addresses combined with the date and time of access can identify the internet users. If there is no such data, it is difficult to identify criminals. Moreover, according to criminological theory - the Deterrence Theories, “criminals are afraid of law and law enforcement or being arrested if they commit crimes. Therefore, criminals will do no crime if there is stringent law enforcement, laws with severe enough penalties, or the possibilities to commit crimes are slight”. Therefore, if service providers are uncooperative to provide information that can identify criminals, the investigation to identify cybercriminals is difficult. Accordingly, criminals are not afraid of laws and continue to commit crimes. The aforementioned result is also consistent with the previous study that the problem of cybercrime investigation is partly caused by the lack of cooperation between public and private sectors that have duties related to technology (Siripongwattana & Pakdeenarong, 2015). Furthermore, officers lack technological knowledge. This results in that knowledge cannot be extended and the agency is ineffective. This is also consistent with the research of Dechsakul & Trimek, 2019 indicated that the justice process in respect of prosecution in cybercrime cases is delayed due to unspecialized and inadequate officers and the difficulty of collecting evidence that needs to seek from the outsource and private sectors as well as various equipment and technologies are lacked to track the accused (Dechsakul &Trimek, 2019).

The research revealed that police cooperation on cybercrime that has been developed by additional training will enhance the efficiency of cybercrime investigation and meet the demands of completed cybercrime investigation due to cybercrime investigators’ perceptions of various organizational patterns and educational backgrounds. Consequently, this will help the development of cybercrime investigation training (Leppänen & Kankaanranta, 2017). This is consistent with research results that the cybercrime investigation of officers is quite ineffective due to the lack of knowledge. Therefore, if cybercrime investigating officers are additionally trained, they will understand investigation techniques that can be developed for the more effective gathering of evidence in the investigation.

Regarding the model of cybercrime investigation in fraudulent cases, the aforementioned model is consistent with the principle of crime deterrence according to deterrence theories that criminals are afraid of laws and law

enforcement or afraid of being arrested if they commit crimes. Therefore, criminals will do no crime if there are stringent law enforcement, laws with severe enough penalties, or the possibilities to commit crimes are slight. The theory emphasizes the significance of the "possibility" to commit crimes. These theories can be concluded that effective crime prevention requires measures or approaches to reduce the possibilities of criminals committing crimes because general criminals commit crimes without considering the benefits which they will obtain after committing crimes. Criminals sometimes commit gang-robbery or robbery and get only small properties. Yet, they will be afraid of committing crimes if they have considered that there is a high possibility to get arrested or there is no possibility to commit a crime. Therefore, effective measures to prevent crimes must minimize the possibilities of crime. As studied the model of cybercrime investigation in fraudulent cases, the figure of CHERRY MODEL is created showing various elements that make investigation successful as follows:

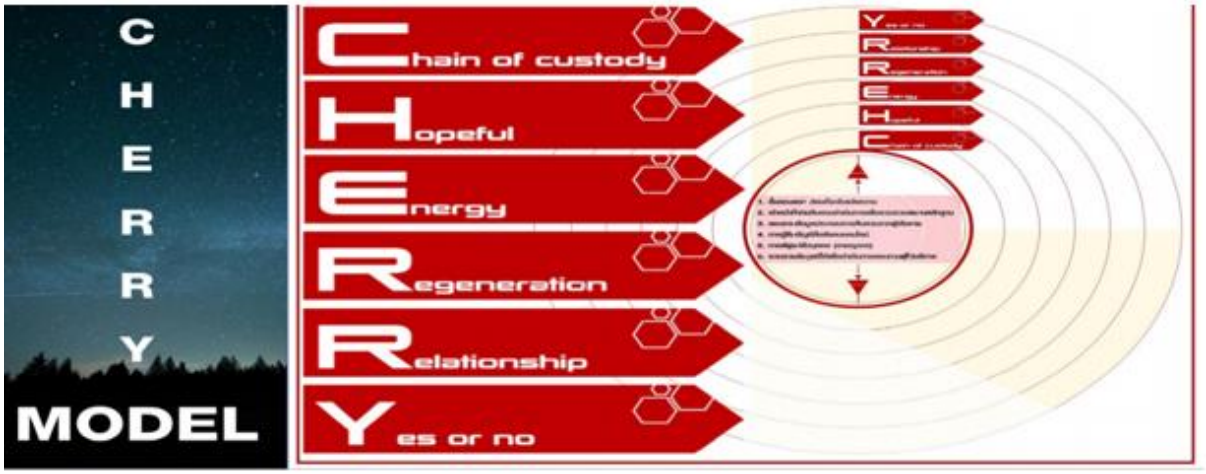

Figure 2 Elements causing the success of the investigation

According to the previous figure, CHERRY MODEL comprises Chain of custody,

Hopeful, Energy, Regeneration, Relationship, and Yes or No with the following descriptions:

Table 1

Definition of CHERRY MODEL

Letter	Vocabulary	Meaning
C	Chain of custody	Officers must maintain the reliability of evidence in order to be useful in the investigation
H	Hopeful	Officers must be hopeful for the success of cases so that the objective will be clear and can see the success of solution of cases
E	Energy	Officers must be energetic to solve problems and love their own duties
R	Regeneration	Officers must take to effort to spread knowledge and regenerate investigator to remain and develop knowledge
R	Relationship	Coordination of information used in the investigation in neighboring agencies
Y	Yes or No	To enhance immunity to people to be aware of, and prevent people from being victimized

This research aimed to study problems of cybercrime investigation of law enforcement officers in order to suggest the model management of cybercrime investigation in fraudulent cases. The research revealed that problems of cybercrime investigation are caused by law enforcement agencies and officers. That is agencies that are in charge of suppression of cybercrime lack forces, technologies, and maintenances and have no preparedness when compared to workloads. Besides, there are problems of distributing duties within the agency and also a lack of cooperation from technology service providers. The model management of cybercrime investigation in fraudulent cases comprises inquiring and explaining information before receiving a report,

investigating officers gathering information, inquiring of victims about information supporting the investigation, recovering social media account, identifying (criminals), and gathering acquired information to submit a request for information from service providers. According to the research of model of cybercrime investigation in Thailand: importing false data into a computer system cases, there are interesting suggestions as follows.

The government should emphasize every relevant information in the cybercrime investigation processes. Therefore, the coordination center should be urgently established and directly subordinate to the Prime Minister. Besides, agencies with cybercrime-related duties should be allowed to fully utilize this center. For a request for information to prove the guilt of offenders, there should be a central agency for requesting information where law enforcement officers are able to cooperate and request for information at all times in order to use in the investigation. In addition, request for such information requires reliable certifying officers. Also, the Royal Thai Police must issue regulations or laws regarding the performance of duty that officers are able to disburse the money for performing duty and do not need to use their personal money. Additionally, for office equipment and programs for investigation and performance of duty, there must be regulations requiring investigating officers to perform duties together with inquiry officers by organizing the investigating officer on duty to sit together with the inquiry sector and jointly gather evidence and find solutions for victims. Furthermore, the Department of Special Investigation should establish the investigation institution and program to be equivalent to the Royal Police Cadet Academy. For officers of the Department of Special Investigation, those who have bachelor's degrees can directly join the Department of Special Investigation in order to achieve corporate culture and eliminate the problem of not accepting each other due to recruiting from various agencies to become officers of the Department of Special Investigation

References

[1] Borwornchai, D. (2020). Knowledge management about investigative work that is the best practice of the detective 4.0 era. Journal of Arts Management, 4(2), 385-398, from https://so02.tci-thaijo.org/index.php/jam/article/view/241505

[2] Braga, A. A., Flynn, E. A., Kelling, G. L. & Cole, C. M. (2011). Moving the Work of Criminal Investigators Towards Crime Control. U.S. Department of Justice presorted standard. https://www.ojp.gov/pdffiles1/nij/232994.pdf

[3]

[4] Chen and Burstein. (2006). A dynamic model of knowledge management for higher education development. March 19, Retrieved From https://ieeexplore.ieee.org/abstract/document/4141625

[5] Dechsakul, N. and Trimek, J. (2019, May 1). Online shopping fraud in Thailand. https://rsucon.rsu.ac.th/files/proceedings/nation2020/NA20-090.pdf

[6] Harkin, D., Whelan, C. & Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. Police Practice and Research: An International Journal, 19(6), 519-536. https://doi.org/10.1080/15614263.2018.1507889

[7] Holt & Bossler. (2012). Cybercrime training and investigation in selected United States Police Departments. Cyberpsychology, Behavior, and Social Networking, 15(9), 464-472. http://doi.org/10.1089/cyber.2011.0625

[8] Khantee, P. (2015). Criminological theory: principle, research and policy implication. Bangkok: Rangsit University

[9] Leppänen, A. & Kankaanranta, T. (2017). Cybercrime investigation in Finland. Journal of Scandinavian Studies in Criminology and Crime Prevention, 18(2), 157-175. https://doi.org/10.1080/14043858.2017.1385231

[10] Leukfeldt, R., Veenstra, S. & Stol, W. (2013). High volume cybercrime and the organization of the police: the results of two empirical studies in the Netherlands. International Journal of Cyber Criminology 7(1), 1-17. https://www.researchgate.net/publication/280013987_High_Volume_Cyber_Crime_and_the_Organization_of_the_Police_The_results_of_two_empirical_studies_in_the_Netherlands

[11] Maslow, Abraham H. (1980). Theory of Human Motivation (2nd ed). New York: Harper and Rows Publisher.

[12] Oonjai, D. (2020) Quality of work life of police in Chana Songkhram Metropolitan Police

[13] Station. Journal of Crime and Security, 2(1), 9-16, from https://so06.tci-thaijo.org/index.php/jcs_rpca/article/view/243087/164855

[14] Pisarić, M. (2015). Specialization of criminal justice authorities in dealing with cybercrime. Journal of Criminal Justice and Security, 17(2), 230–242. https://www.fvv.um.si/rV/arhiv/2015-2/07_Pisaric_rV_2015-2.pdf

[15] Police Executive Research Forum. (2018). New national committee required: the changing nature of crime and criminal investigations. Police Forum. https://www.policeforum.org/assets/ChangingNatureofCrime.pdf

[16] Saruang, S. (2019). Crime on internet. Interdisciplinary Studies Journal, 18(2), 135-161, from https://so02.tci-thaijo.org/index.php/sahasart/article/view/220418/152356

[17] Siripongwattana, N. and Pakdeenarong, P. (2015). Development of computer crime of the Royal Thai Police and Department of Special Investigation. Suan Dusid Graduate School Academic Journal, 11(3), 85-93, from http://www.graduate.dusit.ac.th/journal/index.php/sdujournal/article/view/332

[18] Sun, J.R., Shih, M. L. & Hwang, M.S. (2015). A Survey of digital evidences forensic and cybercrime investigation procedure. International Journal of Network Security, 17(5),497-509. http://ijns.jalaxy.com.tw/contents/ijns-v17-n5/ijns-2015-v17-n5-p497-509.pdf

[19] Sutriyanitipakdee, T., Techagaisiyavanit, W and & Borwornnuntakul, T. (n.d.). Computer crime a case study of the prevention of unauthorized access to the computer system. http://acad.vru.ac.th/acad_journal_online/journalFile/datajournaP220.pdf

[20] Thailand Emergency Response Team. (2020). Threat statistics for the year 2019. Retrieved from https://www.thaicert.or.th/statistics/statistics.html

[21] Wayupap, S. (2019, September 30). Young age, old age, smart and know the internet. Retrieved from http://www.mnst.go.th/computer/index.php/2019/09/30/ebook/

[22] Wu, Y., Xiang, D., Gao, J. M. and Wu, Y. (2019). Research on investigation and evidence collection of cybercrime Cases. Journal of Physic, 1176(4), 1-7. https://iopscience.iop.org/article/10.1088/1742-6596/1176/4/042064/pdf