www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Cyber Crime Triangle Approach to Encounter Cybercrime

Sri Sundari[1], Muhammad Haikal Kautsar[2]
[1,2]*Universitas Pertahanan, Komplek IPSC Sentul, Indonesia*
sri.sundari@idu.ac.id

Abstract

This study anlyze and discuss problem in encounter of cyber crime using crime triangle approach. crime triangle approach is necessary in order to understanding cyber crime from characteristics of crime and offender. This study use qualitative methode that based on non numeric data e.g article and picture. The data filtern and interpreted by understanding the literature. Result of this study explain that there are there element that can be used in order to cyber crime analysis, there are system, provider, and law enforcer. This three element is key factor that can interfere, prevent cracker to commit crime and protect potential victim, and create safe and protected cyber environment. Recomendation of this study law enforcer must be strengthened by creating regualtion that can protect the user of cyber space. This is essential to minimize the number of data theft in the future.

Keywords
cyber crime; encounter cybercrime

I. Introduction

Revolution Industry 4.0 is inevitable in entire the world. Integration of daily life on internet accsess (Internet of Thing) is become part of society. Today, people as if life in two kind of world, first real or physical world; second, digital or inphysical world. In the real life society have so many problem, one of many problem is crime. Crime become concern in society to be minimize in many ways. Crime that common happen in real life is robbery, kidnapped, theft, etc. Meanwhile in real world the problem of crime have not solve, or even never could be solved, the world have to face the new kind of crime that came from cyber space.

Cybercrime itself has grow since 1978, the first spam-mail via arpanet, until now the latest and the biggest cyber attack that happen, wannacry malware that attack hospital and several vital institutions. That phenomenon is indication of the grow of cybercrime in the revolution industry 4.0 Era. Therefore the issues of cybercrime must be handled immediately.

Today the number of internet users is grow significantly, the role of industrial revolution be catalisator to growth of internet penetration. In Indonesia the number of internet users increase exponentially. In 2017 the number of internet users reach 143,26 million people, almost 54,68% of entire Indonesia population (Maulani, 2018). This number show big opportunity for offender to do crime in cyber space, because cybercrime is cheap to commit and expensive to defend.

Therfore, this study see the significant of the priority to review the way to protect people from cybercrime. This study try to elaborate the criminology theory I alternative to analyze and find problems in cybercrime phenomenon. This paper consist five part of explanation, section one section is introduction to cybercrime phenomenon; section two is the definition of cybercrime; section three is the methodology of this study; section four is discussion of modification of triangle theory to understand the cybercrime.

II. Review of Literature

The internet and social media are seen as having the potential to expand public sphere, territory or domain where discourse takes place involving citizens openly. However, the existence of the Internet public sphere tends to be seen as a contestation space where corporate and state forces try with various ways to control and dominate it. Nevertheless, the wave of digital activism has become a creative means for citizens to develop global and local discourses. They use social media as an alternative to creating autonomous public sphere, and consolidate counter power against other forces (state / corporation) (Bo'do, 2019).

2.1 Cybercrime

In this section the study will explain the definition and kinds of cybercrime. As an first step before the discussion of triangle theory. The definition of cybercrime has develop experientially. They differ rely on the perception of observer. and victim and are partly a function of computer-related crime geographic evolution. The Council of Europes Cybercrime Treaty define Cybercrime as offences ranging from criminal activity againts data to content and copyright infingement (Krone, 2005). Meanwhile, Zeviar-Geese suggest that the definition is broader, including activities such as fraud, unauthorized access, child phornography, and cyberstalking (Zeviar, 1998). The United Nation Manual on the Prevention and Control of Computer define cybercrime is relaed crime includes fraud, forgery, and unauthorized accsess (Uniterd Nation, 1995). Gordon and Ford (2006) define cybercrime more general, as they define that cybercrime is any crime that is facilitated or committed using a computer, network, or hardware device (Gordon & Ford, 2006).

By the definiton of three expert that explain before, the researcher try to conclude that cybercrime is any kind of crime that happen in the cyberspace and impact to real space and have implication to economics or value loss. There is a lot of kind of cybercrime, therefore Gordon and Ford (2006) subdivide cybercrime into two distinct types; Type I and Type II cybercrime. Each type of cybercrime as own definition and example of the crime that include. This division is helped researcher to selected the crime is categorize as cybercrime or not.

Cybercrime Type I has several characteristics according to Gordon and Ford (2006):

1. It is generally a singular, or discrete, event from the perspective of the victim
2. It often is facilitated by the introduction of crimeware programs such as keystrokes loggers, viruses, rootkits, or trojan horses into the user's computer system.
3. The introductions can, but may not necessarily be facilitated by vulnerabilities.

A single event or discrete instance, from the user's perspective, might look something like this:

1. The user goes online to perfrom a task, i.e access the WWW, or read/reply to e-mail.
2. User takes actin which then allows the criminal access to information (entering personal information on the look-a-like site, (or) clicks on some object resulting in the download of a Trojan or keystroke logger.
3. This information is used by attecker/
4. The user becomes aware of the crime – this is the single event from ther perspective of the user/ this usually occurs much later in the lifecycle of the cybercrime.
5. The crime is investigated and resolved

This type of cybercrime requires theat data be protected from traditional threats, but also that users be cognizant of the cocept of "vulnerabilites" (Gordon & Ford, 2006). Then, cybercrime Type II, has different approach to see the crime activity that happen in cyber space. Cybercrime Type II is crime activity that the crime is commited by the person organization not by ware. The example of cybercrime Type II is cyberstalking, child predation, extortion, blackmail, stock market manipulation, espionage, or terrorist activities online. According to Gordon and Ford (2006) the characteristic of Type II cybercrime are that;

1. It is generally facilitated by programs that do not fit under the classification cimeware.
2. There are generaly repeated contacts or events from the perspective of the user.

Understanding cybercrime types is important to identify the concept crime that can be modificate in Crime Triangle theory. Researcher will focus on type II cybercrime especially, data theft.

2.2 Place and Triangle Crime

This paper used Crime Triangle theory to explain the phenomenon of cybercrime. Crime Triangle theory is initiated John E. Eck in 1995 as a development of Routine Activity theory that published in 1979 by Cohen and Felson. Triangle theory develop the Routine Activity theory by proposing a third type of crime controller. The theory suggest that crime will occur then offenders and targets converge in places there all three controllers – guardians, handlers, and managers – are ineffective, absent, or negligent (Madensen, 2010). In Crime Triangle theory there are thre element of crime there are, offender, place, and target/victim. While to encounter the crime according to Crime Triangle theory there are there element that can intevent the crime action, Handler, Manager, and Guardian.

III. Research Methods

This study use qualitative approach, which is based on non-numeric data such as article and picture, and filtration of data is done for interpretation from literature review (Creswell, 2003). Review sources from Journal, Report, Books, and article from reliable sources. This study review the Crime Triangle theory and modify to explain in cybercrime phenomenon.

IV. Results and Discussion

In this section researcher will explained why cybercrime could happen using the Crime Triangle approach. As the first step of the discussion researcher will explain the definition of each element of crime triangle. Cybercrime could happen if this three element available, Cracker,Victim, Cyber Space. This element bound each other in order to commit crime. If one of this element absent the crime will not happen.

In this study we use cracker to represent offender in cybercrime. The number of potential cracker growth with the number of internet penetration, because the number internet user and cybercrime has a big relationship (Methmali, 2016). "Cracker" is the term that researcher use to represent offender in cyber space. The reason why researcher use term "cracker" to represent offender rather than "hacker" is "hacker" is person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes

within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage data. However, "cracker" s one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data, deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious (Anonymous, 2002).

Then, the cracker in cybercrime is someone who illegaly access the intellectual property rights and privacy to people or organization who used electronic devices to commit data theft. The shifting of crime incident from real life crime to cybercrime is because criminals operate within the virtual environment and as such are not constrained by real world boundaries by using electronic devices and internet. It's not by chance that they exploit the widely differing legal and regulatory regimes in place within different countries (McMurdie, 2017). Cracker in cybercrime is very difficult to identify, because it could be anyone and anonym. In cybercrime the people who we consider as victim could be cracker or the guardian that we consider to be protector could be craker too.

Next element of crime action is victim. In cyber world everybody can be victim and cracker. But, consider a lot of people is unable to do some hacking action, so the number of probability to be victim is larger than become cracker. The potential victim in cybercrime is usually person or organization that have daily activity with electronic that connected to internet. They daily activity working, studying, shopping on electronic devices e.g smartphone, tab, or computer become new habit for people in the world besides activity in the real world. The big number of internet users makes the internet users as potential victim. Different with victim of real life crime, victim of cybercrime could be hard to identify. It is because some people use two or more electronic device, it means they double chance and fragile to be victim of cybercrime.

Then, one of the most element that become essential factor to crime occur is cyber space. different with real space, cyber space has no physical boundaries, no owner, no real citizen. Therefore, crime could be happen any where and any time. In cybercrime places can take place both in cyberspace and real space, but every cybercrime is always happen through cyberspace. Cyberspace is the name of a real non-space world, which is characterised by the ability for virtual presence of, and interaction between, people through icons, waypoints and artificial realities (Fourkas, 2004). So the cracker will more freely to do crime and the victim become more vulnerable.This is make some offenders choose to use cyber space as place to commit crime cause it is very wide, very fragile, and very cheap. It is more easy to stole data from database online rather than to infiltrate to the administration centre to physical document.

In this era every device that integrated to the internet have possibility to be victim of cybercrime. In this study the cybercrime case that we will discuss is data theft. It is because data theft is have economic and bargaining value to be stolen by the hacker. A lot of industry use stolen data to be used in blackmail, marketing, spionage, etc. It is proved by the phenomenon that several privacy data is sold in order to achieve marketing target (Sukmana, 2019).

When all this three component is fulfill the crime could be occur. But, there is another triangle that could prevent and encounter the crime to be happen. We call it triangle of intervening. This triangle have three element consisting of System, Provider, and Law Enforcer. Every element has role to intervent the triangle of crime. we will explain the role for each element.

Security system is the one ot three aspect to prevent cybercrime happen. Security system has role to protect the data from mailware, spyware, viruses, and security breaching. System in this era could run automatically without supervised of human. Therfore it can work 24 hours stand by to protect the user of electronic devices. The example of security system is firewall, antivirus, antispyware, and encryptionware. The availability of firewall and antivirus can help protect the user from inflitration of unwantedware that can stole the data. The absent of of security system makes the user fragile and vulnerable. In the case of data theft if the user is realize that they vulnerable, they will improve the security system to protect they worthy data.

If we refer to crime triangle theory there is owner of place or manager that have role to prevent the crime to be occured. In cyberspace there is no physical boundaries and real place, therefore the concept of land owner changes to technology provider. Technology provider is organization or institution that provide the technology to be used by people in order to get in touch to cybercommunity and space. The example of technology provider are internet provider, server provider, search engine provider, etc, they have role to prevent cracker to do crime by providing high and secure technology to customer. When the technology provider do not prepare the proper technology to prevent any crime, the cracker can commit the crime, e.g. paypal as mobile payment pioneer if they could prove proper technology to protect the customer. The privacy and property of customer could be stolen by cracker.

The last component is The Guardian. The concept of guardian in cybercrime is law enforcer institution that have responsibility to protect people from cybercrime. It seems have similiarity to the concept of guardian in real Crime Triangle theory, but the different is in real Crime Triangle concept the guardian tend to institution or people who have physical power or weaponary as tool for protect, e.g police, military, security guard, etc. Meanwhile in cyberspace the law enforcement is not someone who have weaponary, but institutons who have legitimitae to punish, to create a law, and to create a system, e.g in Indonesia they have National Cyber and Crypto Agency (BSSN) as law enforcer to protect netizen, people in cyberspace, from the potential cracker that can interfere national interest of Indonesia. When the law enforcer role is absent the cracker can commit crime freely without any hestitate. Because they know that the regulation is unable to punish them and the law enforcer doesn't have obligation to bring them to trial.

The number of data theft in Indonesia is in 945 case in first quarter 2018 and 1162 case in 2017. Approximately 4,5 million data has been stole in first quarter 2018. Number of data breaching each day estimate 6,9 million data. The number of data theft report from 2013 to 2018 is 14,6 Million. The percentage of data lost is 56,11 percent from media social company and 26,62 percent from government institutions. Related to the cause of data breaching, 56,08 percent cause by malware from external party. Meanwhile data breaching caused by accidentally activity is 33,6 percent (Wardani, 2018). From the phenomenon that researcher mention the fact of malware can steal the data is because the weak security system and lack of awarness from the provider to protect their customer data. The absent of this two component could lead the data theft action (cybercrime).

Researcher argue that the most essential aspect that influence to the high number of data theft in Indonesia is the lack of regulation that protect personal data. The constitution have not regulate the law of data protection strongly. Researcher try to review the latest case that afflict one of the biggest marketplace in Indonesia. A cracker from pakistan Gnosticplayers claim have stole customer data from the victim (marketplace). The Ministry of Communication and Informatics admit that it is difficult to bring the cracker to trial. Acting Head of Public Relation Bureau state that we have not the constitutions to bring the

privacy data breacher to trial. Besides the Information and Electronic Transaction act have not examine and rule the case of privacy data theft in detail (Satriawan, 2019).

That phenomenon can be interpret from cracker perspective is a big opportunity to commit crime. they could commit cheap and hassle-free crime action. Besides the value of the data is very worthy economically. If the law enforcer not responsive immediately this phenomenon by speed up the formulation of the regulation, in the future the number of data theft will increase concomitant the increase of internet users. Also from this phenomenon we can syntesize, even the system is already strong enough, the marketplace provider already concern about data protection, if there is no strong law enforcer (regulation) to protect victim, it could not prevent crime to happen. Therefore researchers illustrate the Cybercrime Triangle to explain the cybercrime case we show in figure 2 below:

Figure 1. *The Cybercrime Triangle*

The first inner layer of the triangle lists the three elements that must be present for a cybercrime to occur, while the outter triangle represents the controllers that may intervene on behalf of each element to prevent crime from occuring. Law enforcer will protect the target/victim generally by tools that they have, regulation, power, and facility. System will protect target/victim closely, personaly, and customly, they prevent cracker to penetrate to data or private object of victim. Provider is “landlord” of cyberspace they provide facility for people to access the cyberspace. They can facilitate both cracker to commit crime or protect victim.

In the end, Analyses based on the crime triangle could help stakeholder of cyber world to examine the characterics of the three elements and three controllers related to a spesific cybercrime problem. Interventions to reduce the cybercrime are then developed by considering whether one or more of the three elements can be altered or removed.

V. Conclusion

To conclude this study, the development of cyber security can be built by using cybercrime triangle approach. This paradigm help the stakeholder to focus the development on main three element to interfere the cybercrime law enforcer, system, and provider. The interfere element could protech the victim, prevent the cracker to act, and create safe and secure cyber space environment. Suggestion from this study is for improvement cyber security in Indonesia, researchers suggest that it is necessary to speed up the discussion and formulation of data protection law in Indonesia. This is possibly could minimize the number data theft case in the future.

For future research, researcher suggest to improvement of the theory by exploring another element to enlarge possibility that cause cybercrime. Future research could looking for some statistical evidence to support the concept of Cybercrime Triangle.

References

Anonymous. (2002). The Difference Between Hackers and Crackers. In Anonymous, Maximum Security. Que.

Bo'do, S., et al. (2019). Social Media, Public Sphere and Movement Discussion of Urban Farming in Indonesia. Budapest International Research and Critics Institute-Journal (BIRCI-Journal). P. 250-261.

Creswell, J. W. (2003). Research Design Qualitative, Quantitative, and Mix Methods Approaches (2nd ed). California: Sage Publishing.

Fourkas, V. (2004). What is Cyberspace. Media Development.

Gordon, S., & Ford, R. (2006). on the definition and classification of cybercrime. Journal of Computer Virology, 13-20.

Krone, T. (2005). High Tech crime brief. Canberra: Austria Institute of Criminology.

Madensen, T. (2010). Eck, John E: Places and The Crime Triangle. Thousand Oaks: Encyclopedia of Criminological Theory.

Maulani. (2018, February 20). Internet penetration in Indonesia reaches 143M people: APJII ReportE. Retrieved from E27: https://e27.co/internet-user-penetration-indonesia-reaches-143m-people-report-20180220/

McMurdie, C. (2017, August 21). Cybercrime: Cheap to commit and Expensive to Defend. Retrieved from Knect365: https://knect365.com/superreturn/article/44f8a805-4757-4659-a3bb-461cdde190bd/cyber-crime-cheap-to-commit-and-expensive-to-defend

Methmali, S. (2016). Perception of Internet usage and its impact on cyber-crime in Sri Lanka. International Conference on Signal Processing, Communication, Power, and Embedded System (pp. 674-690). paralakhemundi: Centurion University.

Satriawan, I. (2019, March 18). Ternyata Ini Alasan Sulitnya Bawa Kasus Pencurian Data ke Pengadilan di Indonesia. Retrieved from Bangkapos.com: http://bangka.tribunnews.com/2019/03/18/ternyata-ini-alasan-sulitnya-bawa-kasus-pencurian-data-ke-pengadilan-di-indonesia

Sukmana, Y. (2019, May 13). Data Pribadi Dijual Bebas, dari Gaji hingga Info Kemampuan Finansial. Retrieved from Kompas.Com: https://money.kompas.com/read/2019/05/13/081753626/data-pribadi-dijual-bebas-dari-gaji-hingga-info-kemampuan-finansial?page=all

United Nation. (1995). United Nation: The United Nation manual on the prevention and control of computer related crime. International Review of Criminal Policy.

Wardani, A. S. (2018, Oktober 12). 4,5 Miliar Data Dicuri Selama 6 Bulan Pertama 2018. Retrieved from Liputan 6: https://www.liputan6.com/tekno/read/3665291/45-miliar-data-dicuri-selama-6-bulan-pertama-2018

Zeviar, G. (1998). The State of The Law on Cyberjurisdiction and Cybercrime on the Internet. Gonzaga Journal of Internasional Law.