INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND ANALYSIS

ISSN(print): 2643-9840, ISSN(online): 2643-9875

Volume 07 Issue 11 November 2024

DOI: 10.47191/ijmra/v7-i11-33, Impact Factor: 8.22

Page No. 5245-5248

Digital Fraud: Analyzing the Latest Trends and Tactics in Cybercrime

Mujiono Hafidh Prasetyo[1], Ahmad Ainun Najib[2]

[1, 2]Faculty of Law, Universitas Diponegoro, Indonesia

ABSTRACT: Information technology plays an important role, both now and in the future. Information technology is believed to bring great benefits and interests to countries in the world. There are at least 2 (two) things that make information technology considered so important in spurring world economic growth. First, information technology drives demand for information technology products themselves, such as computers, modems, tools for building internet networks and so on. Second, is to facilitate business transactions, especially financial business in addition to other general businesses. Information technology by the countries that are members of the G-8 group is seen as very vital in the future world economic growth, expanding learning opportunities and obtaining information for the world's people.

KEYWORDS: Analytics, Cybercrime, Society

INTRODUCTION

The development of information technology is currently growing rapidly. Seeing this development, it cannot be denied that it can have a negative impact that is no less numerous than the benefits it brings. The new space created is certainly not even if it has a good impact, there are several parties from the millennial generation who are taking advantage of it to commit a crime known as cybercrime. The worrying thing about the ever-changing development of information technology and the rapid development of software is that security is a very crucial issue and everyone risks time and money to protect privacy data on the internet. The potential for data-related crimes is very likely to occur. Several countries have long paid more attention to the security of data in cyberspace. The implementation of this concern is contained in national regulations related to information technology. Indonesia stipulates all rights and obligations related to cyber law in Law Number 19 of 2016 on Electronic Information and Transactions, abbreviated as the ITE Law.

USE OF INFORMATION TECHNOLOGY IN INDONESIA

Indonesia is one of the countries with the largest population in the world. Judging from the Worldometers website, Indonesia is ranked 4th with a total of 266,794,980, below the United States, India and China. Supported by the increasingly wide range of internet services, as well as the cheap prices of devices supporting internet use such as smartphones, personal computers, tablets, laptops and so on, users of Information Technology devices are growing rapidly in Indonesia. Based on the website katadata.co.id, the number of internet users in Indonesia in 1998 only reached 500 thousand, very far compared to 2017 which reached more than 100 million users. According to survey data from APJII (Association of Indonesian Internet Service Providers), internet users in Indonesia in 2017 reached 142 million people or 54.69 percent of the total population in Indonesia. Internet users in 2016 grew 7.9% from the previous year and grew more than 600% in the last 10 years.

INTRODUCTION OF CYBERCRIME

Cybercrime is a new crime that emerged as a result of the development of Information Technology. Cybercrime involves computers in its implementation. Crimes related to the confidentiality, integrity and existence of data and computer systems need special attention, because these crimes have a different character from conventional crimes. However, according to other research, the means used are not only computers but also technology. So, with the very rapid development of technology in Indonesia at this time, especially Information Technology, it makes.

Digital Fraud: Analyzing the Latest Trends and Tactics in Cybercrime

Cybercrime is one of the cases that we really have to pay attention to and be wary of. Because after all, crimes like this will definitely occur in a region or country. It depends on how a region or country tries to handle it. Cybercrime Cases in Indonesia. As time goes by, Cybercrime cases are increasingly common in all parts of the world, including Indonesia. The emergence of several cases of "Cyber Crime" in Indonesia, such as embezzlement of money from banks via computers, cases of pornographic videos uploaded on the internet, hackers, carding or crimes committed to steal other people's credit card numbers and use them in trade transactions on the internet, the spread of viruses on purpose on the internet, cybersquatting which is defined as registering, selling or using domain names with the intention of taking advantage of other people's trademarks or names via the internet and cases of theft of state leaders' documents via the internet, all of these cybercrime cases show symptoms of shifting social problems in the world real.

In practice, this crime uses sophisticated telematics technology that is difficult to see and can be committed anywhere. The modes and motives of cybercrime are increasingly complex, therefore there is no guarantee of security in cyberspace, and there is no computer security system that hackers will continue to try to conquer the most sophisticated security systems, and it is a satisfaction for hackers if they can break into other people's computer security systems. Through the site published by forbes.com, with the article title "The Top Cyber Security Risks In Asia-Pacific In 2017" it was written that in March, a ransomware variant known as KimcilWare was seen targeting websites running the Magento eCommerce platform. This variant is thought to have been developed in Indonesia. Apart from that, it was also stated that perpetrators from Asia Pacific were very active in carding activities (trading credit cards with other people's bank account details).

The tactics, techniques and procedures (TTPs) involved in carding are being shared both in closed groups on Facebook and in deep web forums. Hackers from Bangladesh, Pakistan, India, Philippines and Indonesia were observed to be the most active in this regard. According to a survey conducted by one of the computer security applications, namely Norton, which was uploaded on its official website, it was stated that in the last year more than 978 million adults in 20 global cybercrime countries experienced cybercrime, one of which was Indonesia with a total of 59.45 million adults. who are the perpetrators of cybercrime. And as for the losses, don't worry as Norton also mentioned, the total loss of consumers who were victims of cybercrime globally, in Indonesia, reached a fantastic value of $3.2 billion. This has explained that Indonesia should be more concerned and understand that cybercrime is a crime that we should be aware of. The more often we connect to the Internet, the greater the possibility that we experience cybercrime. According to one national news article, the most prominent case of cybercrime in Indonesia is hate speech.

In general, both through social media and other means, the National Police handled hate speech cases during 2017 as many as 3,325 cases. Meanwhile in 2016, the Police handled 1,829 cases of hate speech. Not only that, in fact there are still many cyber cases occurring in Indonesia, but unfortunately they still do not receive special attention from the government or the people themselves who are actually the perpetrators and also the victims of these cases, namely the reporting of fake news (Hoaxes). The case of reporting fake news (Hoax) is the case that occurs most often, and is often found around us, every day carried out by our family members, our friends, by the people around us.

Handling Cybercrime in Indonesia

The world faces the same dilemma about how to combat cybercrime and how to effectively promote security to their communities and organizations. Cybercrimes, unlike traditional crimes that are committed in a single geographic location, are committed online and are often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is needed. One of them is Indonesia, the government is now preparing a strategy to deal with Cybercrime cases which are starting to become a special concern at this time.

One of the efforts that the government has made is by establishing the National Cyber and Crypto Agency (BSSN). BSSN, which was formed taking into account the field of cyber security, is one of the areas of government that needs to be encouraged and strengthened as an effort to increase national economic growth and realize national security. The formation of the BSSN is an effort to organize the National Crypto Agency into a National Cyber and Crypto Agency to ensure the implementation of government policies and programs in the field of cyber security. Apart from that, in this case the National Police as the Indonesian law enforcement apparatus has prepared a special unit to handle this cybercrime, namely UNIT V IT/CYBERCRIME Directorate II Special Economics of the National Police Criminal Investigation Unit. The National Police in this case in particular

The cybercrime unit uses parameters based on UN congress documents on The Prevention of Crime and The Treatment of Offenders in Havana, Cuba in 1999 and in Vienna, Austria in 2000, which define cybercrime as an unlawful act committed using a computer network as a means/tool. or computers as objects, whether to gain profit or not, at the expense of other parties. The existence of enforcers is not appropriate without enforced laws.

Therefore, Indonesia also formed a law to regulate Cybercrime, in this case there are 2 main laws used, namely - Telecommunication Law in Law Number 36/1999 and the Information Transaction Electronics (ITE) Law in Law Number 11/2008. According to in-depth observations made by Leo and Dinita regarding the history of cybercrime cases in Indonesia, it shows that the legal basis for cybersecurity is still weak. Compared to other countries, Indonesia lags behind in terms of ICT security policies and regulations. For example, in Malaysia, there is already a Computer Crimes Act, Digital Signature Act, Telemedicine Act (three of them have been in force since 1997), Multimedia Act (1998), Payment Systems Act (2003) and Personal Data Act (2010). Singapore also has a similar set of regulations. Both existing laws have their own limitations. The Telecommunications Law only concerns the scope of telecommunications, but does not mention telecommunications infrastructure, for example in the context of the internet.

So that makes it difficult to put into context specific cases. Apart from that, while a special law on cybercrime has been implemented through Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions (ITE), its scope is also limited, because it still requires other laws to complement it. Due to these limitations, criminal cases related to cybercrimes are being punished under the Criminal Procedure Code (KUHAP Law), Consumer Protection Law Number 8/1999, Copyright Law Number 19/2002 or Anti-Pornography Law Number 44/2008. However, Electronic Information and Transaction Law Number 11/2008 formed the basis for cybersecurity governance related to (and debated) the country.

Even though it is weak in legislative terms, Indonesia is quite strong in terms of technical and procedural steps. International cooperation is also not considered a problem because Indonesia is increasing its international cooperation with various organizations, security experts and forums

to increase its understanding of global threats. As an embodiment of this principle in cybersecurity, Indonesia has become a full member of APCERT and FIRST and a founder of OIC-CERT. As for technical measures, Indonesia has officially recognized compliance with requirements through SNI / ISO / EIC 27001: 2013 concerning Information Security Management Systems. To increase security awareness and track progress, Indonesia has its own framework for assessing domestic information security across government agencies.

The KAMI Index (National Information Security Index) evaluates five areas of information security: governance, risk management, framework, asset management, and technology. However, there is still a lot of work needed. The absence of an officially recognized national governance roadmap for cyber security is one of the pressing priorities (ITU 2015). In relation to the implementation of international standards, ITU (2015) notes that Indonesia has not officially agreed to a national cyber security and framework. This also applies to certification. Currently, Indonesia does not have a national cybersecurity and officially approved framework for certification and accreditation of national institutions and public sector professionals. The Indonesian Internet Providers Association (APJII) confirmed this finding by adding that currently existing standards are mostly adopted from regional or international entities (interview, 2016).

Public Awareness of IT Security The increase in cybercrime in Indonesia has led the government and legal authorities to take several precautions to reduce the number of crimes on the internet through changes to laws according to technological developments. Providing material on Computer Ethics in Higher Education and Understanding Internet Security Awareness to users. However, it all comes back to each user of Information Technology to be aware of the importance of securing their data and activities. However, unfortunately the level of user awareness in maintaining IT security is still not high. As published on the Hootsuite.com site, the percentage of Indonesian people's attitudes regarding the role of technology and their perspective on privacy is obtained.

CONCLUSION

Cybercrime is actually a crime that uses computer tools and technology as a medium for its crime, where there are three parties directly involved in the occurrence of the case, namely the police as law enforcement officers, the general public as victims, and the perpetrators. In order to prevent or handle cybercrime cases (which are actually quite dangerous than non-cybercrimes), the involvement of the police and the public is needed. Both parties are needed to be smarter and understand the laws or dangers of a crime than the perpetrators so that cybercrime cases cannot be carried out smoothly by the perpetrators. For the most common cybercrime in Indonesia, namely the spread of hoax news, a strong understanding is needed of the impacts that will occur from this crime, as well as the laws that have regulated it, in order to obtain a special formula to prevent the spread of hoax news from happening again.

REFRENCES

1) J. Clough, Principles of Cybercrime, second edition. 2015.
2) Worldometers.info, “Countries in the World by population,” 2016. Databooks.co.id, “How many internet users in Indonesia,” 2018. Online. Available: https://databoks.katadata.co.id/datapublish/2018/02/20/berapajumlah-pengguna-internet- di-indonesia.Arifah, “Cybercrime Cases in Indonesia,” J. Bisnis dan Ekon., Vol. 18, No. 2, pp. 185–195, 2011.
3) N. Dustri, D. A. N. Aspek, and H. Yang, “Understanding and Anticipating Cybercrime Activities in Daily Online Activities in Education, Government, and Industry and Applicable Legal Aspects,” Snikom, 2014.
4) R. Anto, “Cyber Crime Cases as the Impact of Technology Developments Cyber Crime Cases as the Impact of Communication Technology Developments that Disturb the Community,” no. July, pp. 0–12, 2018.
5) Ali, “Information Crime (Cybercrime) in the Context of Digital Libraries,” vol. V, no. 1, 2012.N. K. Movanita, “This is the Result of the Police's Work in Combating Cybercrime Throughout 2017 - Kompas.com,” Kompas.com, pp. 1–5, 2017.
6) H. Jahankhani, A. Al-Nemrat, and A. Hosseinian-Far, “Cybercrime classification and characteristics,” Cyber Crime Cyber Terror. Investig. Handb., no. November, pp. 149–164, 2014.Budiman, “Optimizing the Role of the National Cyber and Encryption Agency,” vol. IX, no. 12, 2017.
7) P. R. Golose, “The Development of Cybercrime and Efforts to Handle It in Indonesia by the National Police,” vol. 4, 2006.
8) L. K. Nugraha and D. A. Putri, “Mapping the Cyber Policy Landscape: Indonesia,” no. November, 2016.
9) M. Danuri, “Trends of Cybercrime and Information Technology in Indonesia,” no. January, 2018.
10) S. Kemp, “Digital in 2018 in Southeast Asia,” 2018.
11) M. R. Marwan and Ahyad, “Analysis of the Spread of HOAX News in Indonesia.”
12) M. Elvia and D. R. Monica, “The Role of the Police in Combating Criminal Acts of Spreading Hoax News,” 2018.