

Analyses of cybercrime expansion in Indonesia and preventive actions

M Irfan*, M A Ramdhani, W Darmalaksana, A Wahana and R G Utomo

Department of Informatics, Sunan Gunung Djati Bandung State Islamic University, Jl. AH Nasution No. 105, Bandung, West Java, Indonesia

irfan.bahaf@uinsgd.ac.id

Abstract. Cybercrime is a threat in the digital age. Cybercrime is that activities made by the people for destroying organization network, stealing others valuable data, documents, hacking bank account and transferring money to their own and so on. In Indonesia, Cybercrime has become a serious threat hand in hand with the rapid growth of the Internet and of Internet users in Indonesia. In this paper, presented an analysis on the expansion of cybercrime in Indonesia with some cases and its statistics. This paper also suggests the preventive actions to combat against the cybercrime. In the end, hopefully this paper could be a help to future study of cybercrime in Indonesia.

1. Introduction

Internet is the most important things today. Every works was doing by using Internet. Since 2010, Internet user in Indonesia has been increased from 21.1% to 28.1% in the end of 2013 and still continue to grow in many years forward [1]. People use Internet in many aspects of helping their life. Automatic Transfer Machine (ATM) used for taking money, mobile transaction (e-banking), on-line transaction/trading (e-commerce), e-business and e-government are some of example from advantage the Internet that involve many transactions between users. Although, Internet had already become a common platform as the important things for Indonesian in most activities, but the security and privacy issues still become the problems appear and both of them need to be protected in electronic transaction [2][3].

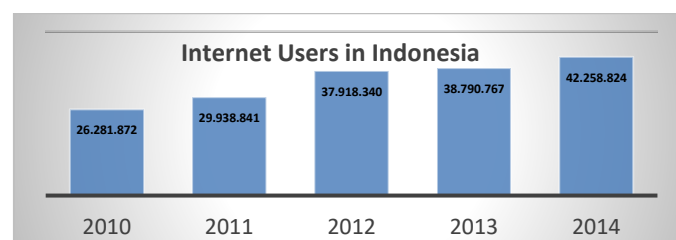


Figure 1. Statistics of internet users in Indonesia (2010-2014).

Cybercrime is regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Cybercrimes describe criminal activity in which the computer or network is necessary part of the crime [4][5][6].



Cybercrime is hard to detect, thus giving the perpetrators plenty of time to flee the area in which the crime was committed. Cybercrimes differ from most terrestrial crimes in four ways [7][8]. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal.

However, defenders have few tools to handle the situation in a timely and effective way. In the cyber space, it is easy to initiate attacks and fly under the radar, and hard to identify attackers and trace back attack sources. The vulnerability of the cyber space firstly roots at the Internet's non-security original architecture design as a private network back to the 1960s. Secondly, as the largest and the most complex manmade system in human history, our understanding of this giant system is limited or even incorrect so far. Thirdly, the anarchism management environment of the Internet is hard for large scale collaboration against cybercrimes. As a result, the cyber space has become a haven for intelligent criminals, who are motivated by significant financial or political reward [9][7][10].

Therefore, this paper provides the expansion of cybercrime in Indonesia including the cases and suggest the prevention to oppose cybercrime acts in Indonesia [11][7].

This paper is divided into five sections. Section I contains introduction to internet users and cybercrime in Indonesia. Section II presents some cybercrime cases that happened in Indonesia. Section III at the statistical data of cybercrime in Indonesia and the analyses of it. Section IV suggests the preventive actions to fight against cybercrime, and Section V concludes this paper with some remarks regarding limitations and suggestions for future research.

2. Indonesia cybercrime cases

Indonesian Computer Emergency Responds Team (ID-CERT) stated that cybercrime can be categorized into several categories: Fraud, Intellectual Property Rights, Spam, Malware, Network Incident, and Spoofing / Phishing [1]. Many cases from that categories has happened and following presented some famous cases which marks the expansion of cybercrime in Indonesia [12][13].

2.1. E-commerce fraud 2001

In 2001, a man from Bandung, Steven Haryanto, made a fake website with internet banking services on purpose to cheat the bank customer [10]. He made many domains with similar name to BCA Bank. He made similar website with www.klikbca.com such as www.klik-bca.com, www.kilkbca.com or www.clikcbca.com. The fake website will guide user if he clicked it to input his identity, username, password and PIN number. Approximation, there are many identity BCA customer has been stolen and so do their money.

This case is a model of typo squatting. Typo squatting is the act to buy and operate many similar domain names with famous domain names and many Internet users can visit his domain from typo of the true website/domain that user wants to visit. The criminals modified the website page for looking as same as the real website. Without conscious, user with wrong typing website name gift what the criminals need such as username, PIN Number, Credit card Number and many privacy data.

2.2. KPU hacked 2004

The event of the penetration took place on April 2004. On Friday, April 16, Xnuxer tried to test the security system kpu.go.id through XSS (cross site scripting) on the IP 202.158.10.117, but screen out the message of risk with a low level (KPU website yet translucent or damaged). It was he doing in his office in Building Danareksa, he became more curious because for a full day KPU website system that really did not successfully penetrated [1].

Saturday, April 17, 2004 at 03.12.42, Xnuxer tried again to penetrate into tnp.kpu.go.id server with SQL Injection and to successfully penetrate tnp.kpu.go.id 203.130.201.134 IP, and managed to update the list of table names party till at 11.23,16 11.34,27. Xnuxer techniques used in the hack through spoofing techniques (misdirection). Xnuxer attacks from IP 202.158.10.117, then open the 208.147.1.1 IP Proxy Anonymous Thailand before entering the IP tnp.kpu.go.id 203.130.201.134, and successfully

opened the display names of 24 political parties contesting the election. Name of the 24 political parties participating in elections later converted into the fruit and animals. Like Partai Jambu, Partai Kolor Ijo, Partai Wirosableng, Partai Kelereng, Partai si Yoyo, Partai Air Minum Kemasan Botol, Partai Dukun Beranak, or Partai Mbah Jambon.

2.3. *Illegal interception telecommunication 2009*

Indonesian shocked by a news from Australian media, based on leaked document from Snowden, the Australian spy agencies have targeted Indonesian President Susilo Bambang Yudhoyono (SBY), the vice-president and other senior ministers for telephone monitoring [11]. The news made a terrible shock for Indonesian government. Because, as a leader of the country, President SBY had very private conversations on his phone and the ministry did have their privacy about country and government too.

Illegal interception is a crucial case. The cases are hard to be traced and solved. Lack of human resource is being an obstacle for Indonesia government. The issue disturbed national security. Indonesian citizens questioned about the safety of Indonesian privacy data. At the point, Indonesian government has no good policy. The action to prevent this kind of case happen again in the future is needed.

3. Statistics of cyber incidents

Based on the annual reports of ID-CERT regarding cybercrime incidents which is based on data obtained and taken out of thirty-seven (37) respondents consisting of: Keminfo, ID-CERT, PANDI, Detik.net, Zone-h and Anti-Fraud Command Center (AFCC), the three telecom operators, seven NAP, and 22 Internet Service Providers (ISP / ISP), a chart can be presented as follows.

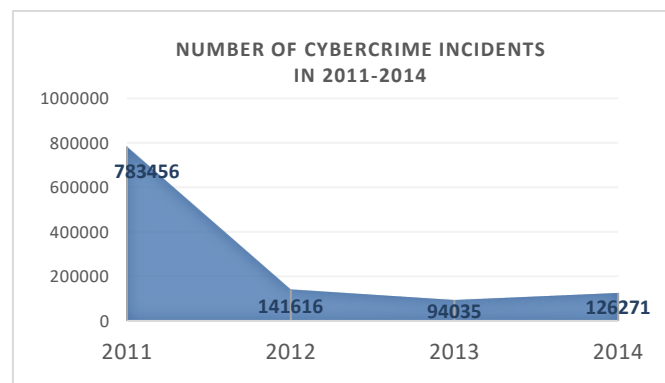


Figure 2. Statistics of cybercrime incidents in 2011-2014.

From graphic on cybercrime incidents in the years 2011-2014 above, shows that the trend of cyber incidents decreased. Starting from the year 2011 that occurred 783,456 incidents then declined in the following year to 141,616 incidents and be 94,035 incidents in 2013, although in 2014 there was a slightly increase of incidents 126,271.

In accordance with cybercrime incident categories, from the data in 2014 which occurred 126,271 cases [6], it can be broken down further more to the number of incidents per category which are presented in the following graphic.

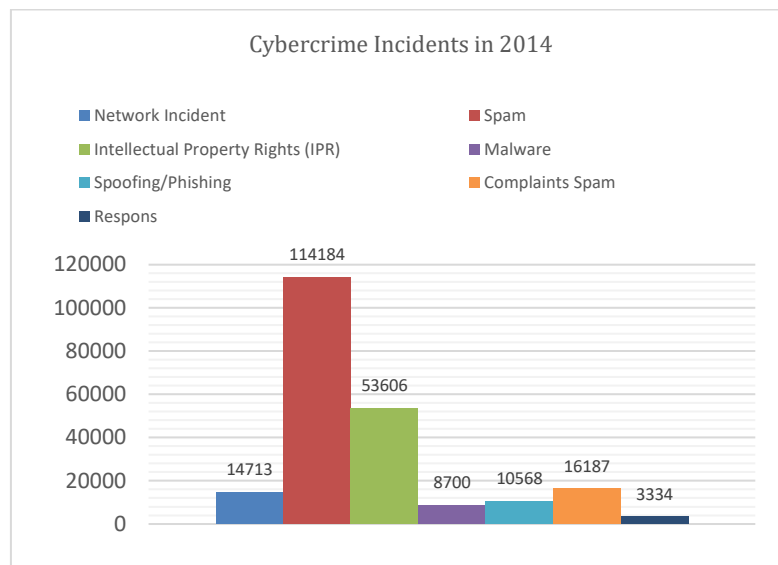


Figure 3. Cybercrime incidents in 2014.

From graphic cybercrime incidents in 2014 above shows that the incident category Spam become the most happened incident with 114184 cases with complaints against spam as much as 16187. Further, infringement of intellectual property rights occurred as many as 53606 adrift far from Network Incident, Spoofing / Phishing and Malware, each of which occurred as many 14713, 10568, 8700 respectively. While the responses to the incidents that happened is still has relatively small number of responses as much as 3334. This proves that the handling of cybercrime cases in Indonesia is still low and prevention is needed so that similar incidents do not happen again and to minimize the impacts.

4. Preventive actions

To protect system or organization from the threats of the cybercrime, there are some preventive actions that can be performed. According to United Nation Office on Drugs and Crime a good crime prevention practice starts with basic principles, suggests forms of organization, and leads to the implementation of methods and approaches [14]. Based on it, Table I presents the suggestive actions that can be used as cybercrime prevention with starts from Cyber Law as a form of basic principle, Special Institution as a form of organization and finally leads to implementation of security methods and approaches to secure the systems [13][15].

Table 1. Preventive actions to oppose cybercrime.

Encryption	Transmitted data is encrypted before transmitted over the internet. On the destination computer, the data is returned to its original form so it can be read and understood by the recipient. This is done so that the attacker cannot understand the sent data.
Firewall	To prevent access from the outside to the internal system. Firewall can work in two ways, namely using filters and proxies. The firewall filters to filter communications to occur only as needed, only certain applications that could pass and only a computer with a certain identity that can relate. Firewall proxy means allowing users to access the internet in the broadest, but from the outside can only access one computer only.
Closing Unnecessary Services	Some services are not used should be closed. This is to prevent threats that take advantage of the gaps are too many services to fit into the system.
System Monitoring	The existence of an attack monitoring system used to determine the presence of guests / someone who was not invited (intruder) or of an attack.
Back Up	Backing up data is done regularly to prevent data loss in the event of an attack that alter or destroy data.
Integrity System Monitoring	The existence of monitoring the integrity of the system. This program can be used to monitor if there is a change in the data or files.
Cyber Law	Cybercrime has not fully accommodated in regulation / legislation that is important to have a special legal instrument given the character of Cybercrime differs from conventional crime.
Special Institution	The institution is needed to provide information about Cybercrime, intensive socialization to the community, as well as conduct research specifically in the response to Cybercrime.
The Use of Closed Telecommunication Media	The Indonesian government and state officials should not use an open telecommunication lines such as Telkomsel, Indosat, etc. in terms of governance and state affairs, but rather uses a closed communication line. The closed nature of telecommunications technology is becoming an anti-tapping.
Audits of Telecommunications Security Periodically	Supposedly audits are conducted regularly and repaired from time to time that there are errors or gaps that could be detected and properly handled.
Vigilance of State Official	Vigilance every state official will be tapping by outsiders needs to be improved and disseminated on a regular basis. Simple ways to determine whether symptoms are being tapped our phones need to be trained and cared for.

5. Conclusions and suggestions

Cybercrime is a threat in the digital age. It cannot be separated from the growth of the internet. In Indonesia, cybercrime become a big threat for government or company. Therefore, for the prevention of the same thing does not happen, the necessary actions to prevent cybercrime acts is need. One of them protective actions for the system to anticipate an attack from inside or outside.

Limitation in this research on the study of cybercrime and its expansion in Indonesia is case study and data. Case study is needed to validate suggested actions to prevent the acts of cybercrime. Furthermore, with the data that are difficult to collected, resulting in the presentation of the specification and cyber-crime in this study is not yet perfected. Hopefully in the future study, the data of cybercrime incidents in Indonesia can be more complete with more sources and this could only happen with the support of various stakeholders to combat against cybercrime.

References

- [1] H S Jannah and M Naufal 2012 Penegakan hukum Cyber Crime Ditinjau dari Hukum Positif dan Hukum Islam *Al-Mawarid* **12** 1 p 69–84
- [2] Undang-Undang Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi **1** 1
- [3] B Sugiantoro and M Mustakim 2017 Analisa Usabilitas Sistem Deteksi Akses Pornografi Pengguna Internet Menggunakan Metode McCall'S, *Join* **2** 1
- [4] U D Negara, R Indonesia and T Lembaran 2106 *UU ITE Nomor 19 Tahun 2016*
- [5] S T C Kurniawan, S Supriyadi and Dedih 2017 Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android *JOIN (Jurnal Online Inform.* **2** 2 p 102–109

- [6] M Irfan, S J Putra, C N Alam, A Subiyakto and A Wahana 2018 Readiness factors for information system strategic planning among universities in developing countries: A systematic review in *Journal of Physics: Conference Series* **978** 1
- [7] V K Gandhi 2012 An overview study on Cyber Crimes in Internet *J. Inf. Eng. Appl.* **2** 1 p 1–6
- [8] D D Bhkati 2016 Pemodelan Sistem Informasi Keuangan Daerah Pada Direktorat Evaluasi Pendanaan Dan Informasi Keuangan Daerah *JOIN (Jurnal Online Inform.)* **1** 2 p 1–6
- [9] E E D Hemdan and D H Manjaiah 2017 Spark-based log data analysis for reconstruction of cybercrime events in cloud environment *Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2017*
- [10] M Irfan 2018 Supply chain management using fp-growth algorithm for medicine distribution *J. Phys. Conf. Ser.* **978** p 012018
- [11] M U R Indonesia 2012 *CYBER CRIME MENURUT UNDANG-UNDANG REPUBLIK INDONESIA* (Perspektif Hukum Pidana Islam)
- [12] R Amalia 2017 *Analisis Yuridis Penegakan Hukum Pidana Terhadap Tindak Pidana Penipuan Bisnis Online*
- [13] M Junger, L Montoya, P Hartel and M Heydari 2017 Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in Europe 2017 *Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, Cyber SA 2017*
- [14] C Onwubiko 2016 Understanding Cyber Situation Awareness *Int. J. Cyber Situational Aware* **1** 1 p 11–30
- [15] G Tsakalidis and K Vergidis 2017 A Systematic Approach Toward Description and Classification of Cybercrime Incidents *IEEE Trans. Syst. Man, Cybern. Syst.* p 1–20