13th International Educational Technology Conference

CYBER SECURITY: RULE OF USE INTERNET SAFELY?

Maskun\textsuperscript{a}, Alma Manuputty\textsuperscript{b*}, S.M.Noor \textsuperscript{c}, Juajir Sumardi\textsuperscript{d}

\textsuperscript{a}PhD Student, Hasanuddin University.
\textsuperscript{b} Professor of Law, Hasanuddin University.
\textsuperscript{c} Professor of Law, Hasanuddin University.
\textsuperscript{d} Professor of Law, Hasanuddin University.

International Law Department
Faculty of Law, Hasanuddin University
Jl. Perintis Kemerdekaan Km. 10, Tamalanrea, 90245, Makassar – South Sulawesi
Manis ck@yahoo.com

Abstract

Cyber security plays on important role to guarantee and protect people who use internet in their daily life. Some cases take place around the world that people get inconvenience condition when they access and use internet. Misuse of internet becomes a current issue which some cases take place including a university. Advantages of using internet in the university of course assist the student to get some information in internet. However, they have to be protected in order to feel convenience when use internet.

Introduction

Internet is becoming an important thing in people daily life and has grown at an explosive rate (Pratap Singh and Bagdi, 2010). According to International Telecommunication Union (ITU) (2013), internet users (population) around the world are over 2.7 billion, which corresponds to almost 40\% of the world’s population. In the
developing countries, people who use internet is around 31% of the population, compared with 77% in the
developed countries (ITU, 2013).

Basically, internet was used to military, defense contractors, and a university research purpose. However, in
recent years, it has been developed to multi-purposes including information, communication, leisure, shopping,
education, e-social activities, financial, job seek, homepage, file share service, and download (Kisa, 2011). Those
internet usage purposes bring both advantages and disadvantages for people and their community. In terms of
disadvantages of internet use such as illegal contents, online fraud, identity theft, espionage, sabotage, cyber
terrorism, and cyberstalking (Boateng, 2011), (Department of Economic and Social affairs, 2012), (Greitzer and
Frincke, 2010), (M. Arif Mansur and Gultom, 2005), (Suhariyanto, 2012), cyber security is therefore needed to
guarantee people who use internet to be safe.

Theoretically, cyber security has to fulfill 3 (three) critical points: measure to protect information technology; the
degree of protection resulting from application of those measures; and the associated field of professional
endeavor (Fisher, 2009). The three critical aspects of cyber security play an important role to protect a personal
data of every person, government, and businesses. Those data are pivotal because they can be misused or
manipulated by other person for criminal purposes.

Internet misuse and manipulation are mostly committed by young and adult people especially people who in level
senior high school and university students. In South Sulawesi for example, some Hasanuddin University students
in 2011 committed financial fraud (Indonesia Hackers, 2011). The crime usually intended to the personal
information stored on personal data forms in computer, such as credit card number and ATM PIN numbers. They
were then arrested by the police and should face suing for their committed crime.

Complexity of definition of cyber security

It is quite difficult to define what does cyber security mean? The difficulty definition arises from several reasons
and tends to be complex. (Fisher, 2009). According to Eric A. Fisher, “there are many components of cyberspace
and many potential components of cyberspace” to be used in order to determine the cyberspace’s meanings.
(Fisher, 2009).

The meaning of cyber security tends to be decided in different context. In some cases, it refers to economic terms
or in social and cultural terms or even in politic and military terms. As it is commonly used, “cyber security
refers to 3 (three) things:

1. A set of activities and other measures intended to protect — from attack, disruption, or other threats —
computers, computer networks, related hardware and devices software, and the information they contain
and communicate, including software and data, as well as other elements of cyberspace. The activities
can include security audits, patch management, authentication procedures, access management, and so
forth. They can involve, for example, examining and evaluating the strengths and vulnerabilities of the
hardware and software used in the country’s political and economic electronic infrastructure. They also
involve detection and reaction to security events, mitigation of impacts, and recovery of affected
components. Other measures can include such things as hardware and software firewalls, physical security such as hardened facilities, and personnel training and responsibilities.

2. The state or quality of being protected from such threats;
3. The broad field of endeavor, including research and analysis, aimed at implementing and improving those activities and quality.” (Fisher, 2009).

According to Rich Rosenthal’s Cyber Assurance Program (Andress, 2011), the complexity of definition of cyber security can be drawn as if:

![Source: Rich Rosenthal’s Cyber Assurance Program](image)

The mapping as shown in figure 1 draws complexity of definition. There are 7 (seven) elements, namely as policy, organization, core, processes, people, skills, and technology, that influence security in cyberspace. Those elements essentially have connection one to another. They have to be developed in one system to create security in the area of cyber space. For example, people as an actor of internet use have intention and skill to use internet in appropriate ways. However, if other elements do not support their intention, it means that they cannot get any advantages from it or otherwise.

According to Andress (2011), some of elements of cyber security issues definition as mentioned in figure 1 are categorized as extremely difficult (ED). They are laws, threat/risk awareness, attribution, deterrence, mission assurance, and resilience and supply chain. Other elements are classified as very difficult (VD) and difficult (D). Classification of those elements actually shows that cyber security plays important role to create “peace” in using internet. Indeed, it is realized that it is not easy-job to reach it.

**Cyber Security: Rule of Use Internet**

Internet user is growing dramatically in variety generation and the purpose of using internet then is done in various ways as explained above. The number of internet users in Indonesia for example is increasing every year. According to Internet World Stats (2010), commercial internet services commenced in Indonesia in 1995 and coming into 2008, Indonesia had an estimated 25 million Internet users. It is predicted that in the beginning of 2013, the number of internet user in Indonesia is becoming bigger than in 2008. Guharoy and Morgan (the Jakarta Post, 2012) furthermore states that internet users in Indonesia is climbing dramatically in the last two years, “20 percent of Indonesians 14 years of age and older now access the Internet every month. That’s over 30
million people, and growing steadily each month. But we need to remember two important facts that characterize the usage. First, roughly 10 of the 30 million users access the Internet via their mobile phones. Second, roughly 70 percent of those 30 million users visit Facebook and twitter each month, making it the most popular address in the country”.

This fact actually is not surprising because computer and its function including internet as introduction have been introduced since the young people in elementary school. It means that the Indonesian young people especially university students have skill to access internet but they are also potentially to misuse or to be misused by the internet. Presence of internet for students in university actually helps them to get a lot of information related to their tasks. The information is provided in forms of book online and journals. Both books and journals give an easy task for the students to finish their tasks particular when they conduct their final paper to be graduated. However, a lot of cases of misuse the internet function also conducted by university students. Plagiarism is one of the most internet misuse conducted by the students. They tend to copy some materials to their tasks but they do not mention the author’s name. Other internet misuse can be found such as illegal contents, online fraud, and identity theft.

According to National Research Council (2003), there are 3 (three) classes of attack that addressed to internet, as following:
1. Service disruption; it causes a loss of service and can result from disabling of networks through a variety of attacks such as denial of service (DoS) and destruction of information.
2. Theft of assets; it misuses critical information on a large enough scale to have major impact.
3. Capture and control; it involves taking control of cyberspace and using them as a weapon.

Those classes of attacks are then classified as cybercrime and also have been modified in various modus. Those modus in fact threaten all human beings activities including infrastructure. To handle and to prevent those crimes, cyber security plays important role to guarantee people to use internet safely.

As we known, cyberspace compiles a huge range of related elements of cyberspace activities and it is therefore cyberspace activities are potentially at risk. To eliminate or dismiss the risk, protection of cyberspace infrastructure is needed in order to stop hackers to commit their crimes. The protection of the infrastructure must cover internet hardware, telecommunications infrastructure, computing devices as control system and computing devices as desktop computer (Fisher, 2019). Andress (2011) furthermore stipulates that to eliminate the risk is not only protection to the infrastructure (hardware) but also must protect the software.

Protection of software is intended to help everybody to use computer/internet safely. It is because so many computers are used in homes and businesses. The computer operating systems and email programs are two aspects of computer/internet that is vulnerable to be attacked and exploited. Case of computer worms that attacked Microsoft Windows operating system in 2003 was a proof to see that the protection of software is needed to protect the internet user (Scheiner); or other sample of a worm (spionage) took place in 2010, when a worm called stuxnet was launched to attack the Iranian nuclear program (Farewell and Rohozinski, 2010).
Both protection of hardware and software are the main point of cyber security. They are able to guarantee people to use internet safely. People will use internet to support their activities without any worry to negative impacts of internet. However, both protections must be implemented and embedded in national and international strategy (regulation) to reach its goals. In United States, for example, it can be found National Strategy for Homeland Security. The purposes of this strategy are to prevent cyber attacks against critical infrastructure; to reduce national vulnerabilities to cyber attack; and, to minimize the damage and recovery time from cyber attacks that do occur (Anonymous, 2003); or another example in Canada, its national strategy is placed on three pillars: securing government systems; partnering with the private sector; and helping Canadians to be secure online through awareness raising (Deibert, 2012).

In terms of Association of Southeast Asian Nations (ASEAN) in which Indonesia one of its members, its regional strategy is put in the area of economic and security cooperative comprised of 10 member nations from Southeast Asia. According to its Roadmap for an ASEAN Community 2009-2015, it has effort to combat transnational cybercrime by fostering cooperation among member-nations' law enforcement agencies and promoting the adoption of cybercrime legislation. In addition, the road map calls for activities to develop information infrastructure and expand computer emergency response teams (CERT) and associated drills to all ASEAN partners (United States Government Accountability Office, 2010). To develop information infrastructure as one of the ASEAN’ roadmap, Indonesia continues to complete Indonesian Law Number 11/2008 Concerning Information and Electronic Transaction. One of its efforts is enacting some Government Decree such as the Government Decree No. 82/2012 Concerning Maintenance System and Electronic Transactions.

Those regulation strategies as implemented in domestic law each country essentially show huge effort of them to create convenience and comfortable environment to internet user to feel safely. Those regulations also must be completed every time to respond some changes related to using internet. So cyber security goals can be reach and are able to eliminate and dismiss negative side of internet usage as discussed above.

Conclusion

Internet has become a global phenomenon; numerous advantages and disadvantages (crimes) are being gotten and committed through the internet. To cope with both advantages and disadvantages, cyber security is needed to guarantee people to use internet safely, particular to young people including university students. Cyber security covers hardware and software infrastructure that is supported by national and international strategy and regulations.

References


