# Computer Crime Prevention in Higher Education Institution Through Computer Crime Act Implementation (UU ITE 11, 2008)

*(A Case Study in the Higher Education Institution in Indonesia)*

Rizki Yudhi Dewantara[1,2]

[1]Student of MPA Double Degree Program at Faculty of Management Sciences
Prince of Songkla University, Thailand
[2]Faculty of Administrative Science-University of Brawijaya, Indonesia
rizkidewantara@yahoo.com

*Abstract* -- The development of communication and computer technology is growing rapidly. Meanwhile computer crime is also developed along with the development of this digital world. The information technology usage in the higher education institution is not immune from computer crime. Higher education institutions collect data from the public for the benefit of educational activities that make the institution also has a strategic data that must be protected, therefore the computer crime law is needed. The Indonesian government has carried out a computer crime law in anticipation of computer crime in Indonesia as well as responds to public anxiety over security in the use of information technology. This paper describes the implementation of the Indonesia computer crime act UU ITE 11, 2008 as a computer crime prevention method in higher education institution in Indonesia

*Keywords: computer crime, computer crime act, information system security, public policy implementation*

## I. INTRODUCTION

Advances in computer technology, information and communication brought new crime that has different characteristics from conventional crime. Crime is estimated using computer technology has led to substantial losses. The speed and efficiency of computer use that benefits the organization also serves crimes using computers. Computer crime is not limited by age, sex, race, as long as the computer has the potential to cause offense, then anyone can commit a crime. For instance reported to the ACFE (Association of Certified Examiners) 755 of the offenders were the main perpetrators and 25% are women. Most of the perpetrators of a crime for the first time, and had no previous criminal record [1]. The motive of the perpetrators of computer crimes are very diverse, ranging from money, for personal pleasure or satisfaction, economic benefits, intellectual challenge, or revenge. In some cases, there may be more than a factor of motivation to commit computer crime [2].

Indonesia already has a criminal record in computer crime since the early 1980s, a bank's computer system was attacked by employees of the bank itself and occurs in state-owned banks. Other forms of computer crime in recent year is the abuse on the Internet, piracy and theft via a website, the spread of pornography and harassment through social networking sites. According to the Association of Indonesian Internet Service Provider (APJII) in 2003, the network has recorded 2267 cases of crimes and in 2004 there were 1103 cases. These cases are not prosecuted by the government and not reported by the victim (www.tekno.kompas.com/read/2008/06/07/15301865). The authorities (police) recorded only two major cases of computer crimes that have been tried in Indonesia. Although many hacking cases occurred in Indonesia, but according to research data Criminal Investigation Police Unit V & Cybercrime IT field, only two cases of successful hacking proven and can be processed to the court, which is the case of website hacking General Elections Commission (KPU) in 2004 and the case hacking website Golkar Party in 2006.

Activities in higher education institutions in Indonesia are dominated by the use of IT, both hardware and software, and computer networks, for which crime can occur. Crimes such as theft, unauthorized access, pornography, sexual harassment, and hacking sites other institutions, can be done through the institutions of higher education. In addition, higher education institutions are not immune from the threat of piracy from the outside because higher education institutions have a strategic data stored in a data center owned by the institution, thus attracting other people want to try to penetrate the computer systems in higher education institutions with various way and motive.

FBI categorizes computer crime are: 1) crimes facilitated by computer, as money laundering, transmission of pornography, or different kinds of fraud; and (2) crimes where a computer itself is the target of the intrusion, data theft, or sabotage [3]. Other than that Laudon also expresses the definition of computer crimes as follow: "Computer crime is the commission of illegal acts stealing valuable Financial Data by illegally Gaining access to a computer system using a home computer [4]".

Computer crimes that occur in higher education institutions such as stealing or modifying data that are confidential, the data could be misused for personal or group of people. Other

cases occur, for example, destroy and destroy important data stored in the data center by breaking through the security of through the use of a computer or against a computer system. Computer or computer system can be the object of the crime (destroying an institution's computer center or an institution's computer files), as well as the instrument of a crime (information systems and spreading the virus so that the user cannot access the data. Based on the information mentioned above, computer systems at institutions of higher education in Indonesia need to be protected from all forms of crime that is happening and will happen. To prevent computer crime, higher education institutions should actively adopt crime prevention measures in the computer information technology systems by applying one computer crime law. This law is the answer from the government as a public policy that needs the security guarantees of all information technology utilization activities. Another activity is to provide knowledge about computer crime or computer crime management training, either to the students or the entire college staff. Application of computer crime laws is not sufficient to prevent computer crime. Since the law cannot walk alone the successful implementation of the Act depends on factors law and several factors on the organization, as a committed and skilled leadership, capacity, and resources of institutions of higher education. State policy of non self-executing means state policy needs to be realized and carried out by various parties so that it looks its effect [5].

This paper aims to describe the contents of UU ITE 11, 2008 and its implementation in institutions of higher education as prevention of computer crime and other forms of crime that use information technology.

## II. METHODOLOGY

The study was conducted in three major cities in East Java province, Indonesia, Surabaya, Malang, and Jember. Those three cities have many institutions of higher education that has a large number of students. The study was conducted at 30 institutions of higher education. Data collection was conducted in March 2012 until August 2012. The research method used is descriptive research method. Descriptive research method is a method of examining the status of the human being, an object, a flashback of events in the present and the purpose of descriptive analysis is to make a description, picture or painting in a systematic, factual and accurate statement of the facts, properties and relationships phenomenon investigated (. Descriptive research is a study that seeks to unravel the issues and circumstances, as they are so as not testing hypotheses. For this type of study is a case study type (case study). The case study is a type of research conducted intensive, detailed and in-depth study of an object in a specific phase of the overall personality. A case study is a research study on the status of the object with respect to a specific phase or typical of the whole personality. The research subjects can be individuals, groups, institutions, or society [6].

Data collection technique that is used was observation, interviews, and documentation. Meanwhile source data obtained from primary and secondary data. Primary data obtained from the department of information and communication technology (ICT Department) in universities, by conducting interviews with department heads, supervisors or chief of staff. Secondary data were obtained from the documents considered important and relevant to the subject matter of the study. Data analysis was performed with a general description such as computer crime, and application of laws ITE 11, 2008 as a public policy in the public and higher education institutions. Further, description of the factors that should be built on the application of computer crime prevention in higher education institutions. The next step is in accordance with the interpretation of the data relevant literature and ends with conclusion.

## III. RESULTS AND DISCUSSION

### A. Research Site

Based on data from the Directorate General of Higher Education in 2011 there were 3172 higher education institutions in Indonesia, higher education classification can be seen in TABLE1. More than 50 percent of higher education is located on the island of Java, because the concentration of the population of Indonesia is located on the island of Java.

East Java is the one of Indonesia's most populous provinces. Based on the data from DIKTI, number of higher education institution in East Java province amounted to 341 institutions and more than 50 percent are located on the three major cities in East Java, Surabaya, Malang, and Jember. (www.evaluasi.dikti.go.id/database/pt).

TABLE I. NUMBER OF HIGHER EDUCATION INSTITUTION IN INDONESIA BY CLASIFICATION

| Classification | Number/Units | Percentage |
|---|---|---|
| University | 477 | 16 |
| Higher School Institution | 1481 | 45 |
| Institute: | 44 | 2 |
| Academy | 997 | 31 |
| Polytechnic | 173 | 6 |
| Total | 3172 | 100 |

Source: www.evaluasi.dikti.go.id/database/pt/2011

### B. Utilization of Information Technology in Higher Education Institutions

Originally, to support teaching and learning activities of students, professors, or researchers can only access resources through print media such as books, journals and research reports, with the rapid development of information technology and tools that such a problem is gone. The existences of digital data center in the college library and the wider source over the Internet helps solve this problem. Moreover, to shorten distance among each user in different countries such as for consult or exchange of research information and teleconference for remote teaching. Such models not only ease communication but also can save on transportation costs by eliminating travel expenses.

The application of information technology in higher education institution is very useful, that is eliminating or reducing barriers or limits of access to sources of information. The entire activities of higher education institutions that use information technology produces Electronic Information, and has been defined in the Act ITE 11, 2008 as defined in article 1 paragraph 1 as follow

"*Electronic Information" means one cluster or clusters of electronic data, including but not limited to writings, sounds, images, maps, drafts, photographs, electronic data interchange (EDI), electronic mails, telegrams, telex, telecopy or the like, letters, signs, figures, Access Codes, symbols or perforations that have been processed for meaning or understandable to persons qualified to understand them."*

The management of higher education institutions also helped by the existence the information technology development; administration and recording of students' academic activities become easier and efficient. Utilization of digital data record has shifted recording data manually, the data was recorded from the first students joined at higher education institutions until the student has graduated and become alumni. Another example is the data of staff both academic staff and the administration staff such as personnel data, payroll, promotions, and the financial and institutional websites entirely recorded on the database center. Some higher education institutions also have built electronic transactions such as tender procurement projects and services, tuition payments, and other transactions using the online system.

Activities or other forms of electronic transactions are also defined in article 1, paragraph 2 that is;

*"Electronic Transaction" means a legal act that is committed by the use of Computers, Computer networks, and/or other electronic media."*

That requires the procurement of information technology, it is defined in article 1, paragraph 3, which;

*" Information Technology means a technique to collect, prepare, store, process, announce, analyze, and/or disseminate information."*

In the observation, all higher education institutions surveyed have used information technology including the use of a computer network system both connected to the Internet or not, therefore the position of higher education in terms of the implementation of information technology has been regulated on the law. In UU ITE 11, 2008 affirmed the position of higher education institutions as providers of electronic systems as mentioned in Article 1 paragraph 6, which

*"Provision of Electronic System" means an Electronic System usage by the state administrators, Persons, Business Entities, and/or the public."*

### C. Kinds of computer crimes that occurs at higher education institutions

Result of interviews with some of the staff and leaders of the information technology department of higher education institutions is known that a computer crime occurs every day in the college environment. Various kinds of computer crimes that occur vary widely both offline and online.

When its offline were:

1. Use of unauthorized user on the user's network system, by providing a user password to others or put a username or password on the computer so that it easier for people who are not eligible to be entered the system. This causes frequent modification of data by unauthorized users or illegally recording confidential data for personal purpose.
2. Spread of the virus by the user because they do not perform antivirus scanning on an external disk (USB) contaminated by the virus.
3. The less physical safeguards to the computer that has access to important data. For example, the lack of security personnel, or the placement of a remote computer that is less monitored by security staff, was resulting in vulnerable from computer theft and vandalism of computer equipment.
4. The use of illegal software, there are many illegal software used in the area of higher education institutions, so that the higher education institutions in the category of computer crimes.

Computer crime that utilizes the internal network and the Internet, such as:

1. Hacking, breach the institution sites or data centers, seeking to change the contents of the website, or destroy data center.
2. Cracking, solving the security code to gain access a database that was secured using passwords.
3. Illegal access to banned sites. Accesses to negative sites are often charged by viruses so harmful the computer system.
4. Utilization of the Internet for things against the law, such as activities that harm others by users in higher education institutions.

### D. Role of Higher Education Institution for Preventing Computer Crime

In order to prevent the computer crime, the higher education institution must apply the Computer crime act to its computer and information system. Effective prevention of computer crime is to apply Act on computer crime. Therefore, higher education institutions that using information technology and electronic transaction shall be implemented based on the principle of the legal certainty and the principle of prudence. As showed in Elucidation of chapter II, article 3 UU ITE 11, 2008 which;

*"Principle of legal certainty" means a legal foundation on which Information Technology and Electronic Transaction usage as well as anything that supports its application shall be legally recognized inside and outside the court.*

*"Principle of prudence" means a foundation on which the parties concerned must address themselves to any aspect with potential for causing damage to both himself/herself and other party in the usage of Information Technology and Electronic Transactions.*

Next clarified in article 15 paragraph 1 that

*Any Electronic System Provider must provide Electronic Systems in reliable and secure manner and shall be responsible for the proper operation of the Electronic Systems.*

*"Reliable" means the Electronic Systems shall have capabilities that match the needs of the users. "Secure" means the Electronic Systems shall be protected in a physical and nonphysical manner. "Proper operation" means the Electronic Systems shall have capabilities that match their specifications.*

Further if the institutions as providers of data access provider, the institution is obliged to apply Article 16 is about the minimum requirements of the operation of electronic systems. The minimum requirements are as follows:

a. *Can redisplay Electronic Information and/or Electronic Records in their entirety in accordance with the retention period as provided for by Laws and Regulations;*
b. *Can protect the availability, entirety, authenticity, confidentiality, and accessibility of Electronic Information in the Provision of Electronic Systems;*
c. *Can operate in compliance with procedures or guidelines for the Provision of Electronic Systems;*
d. *Are furnished with procedures or guidelines that are announced with languages, information, or symbols that are understandable to parties attributed to the Provision of Electronic Systems; and*
e. *Adopt sustainable mechanism in order to maintain updates, clarity, and accountability for the procedures or guidelines;*

Further the government will provide protection to the organizations that have implemented information systems and the protection of critical data. This is regulated in Article 40 paragraph 3-5 states that

*(Paragraph 3) The Government shall specify agencies or institutions holding strategic electronic data that must be protected.*

*(Paragraph 4) Must create Electronic Records and the electronic backups thereof, and connect the with specified data centers in the interest of data security.*

*(Paragraph 5) Other agencies or institutions other than those regulated by section (3) shall create Electronic Records and their electronic backups as necessary to protect data they hold.*

However, adoption the Computer Crime Act is not sufficient to prevent computer crime: Laws are not self-implementing. Successful implementation depends on both law factors and a host of factors, such as the committed and skillful leadership, capacity, and resources of the agencies.

In this paper, the researchers grouped the preparation of the information systems security activities into two parts, administration preparation and technical preparation. Researchers concluded that these preparations to accommodate the application of the Act UU ITE 11, 2008 in computer crime prevention

a. Administrative Control: Some examples of administrative controls include the corporate security policy, password policy, hiring policies, and disciplinary policies that form the basis for the selection and implementation of logical and physical controls. Result of the observation from 30 higher institutions known

   1. Establish a working group, only 30% from institution create working group, all institutions that create the working group putting members from relevant agencies with handling computer crime and has decision-making authority on securing information systems. This working group has regular meetings to discuss issues and cases of computer crime in the institution and evaluate the activities that have been performed by the group. The working group is working to minimize the threat of computer crime in higher education institution.
   2. Furthermore, from the results of observation, 50% of the institutions have information system security policy, but only a few that declare security policy about 7%. Meanwhile, in terms of providing the document relating to the Increase knowledge of computer crimes to all users of the observations obtained results that procurement documents are mostly just for the IT staff (87%) and only a little to the general staff member (27%) and for students (17%).
   3. The results of other observations that 47% of higher education institutions organize training on handling computer crime and security information systems to students and staff of the higher education institution and only 37% conduct training on handling computer crime and security information to staff IT systems.

b. Technical control use software and hardware resources to control access information and computing system, to help mitigate the potential for errors and blatant security policy violation [7].

Almost all of higher education institutions have implemented the security on information systems. But securing information systems is not completely guaranteeing the crimes that may occur. Result of observation are shown in Table 2 gives an overview of the level of security applied to higher education institutions

From these results it can be seen that the antivirus application is the most used of information system protection at higher education institutions. To protect its system against viruses, companies (institution) must buy virus detection software; program that scan computer's disk to detect the virus [8]. The next is applying Intrusion detection system. IDS are a combination of hardware and software that continuously

monitors the traffic. Data backup activity is also very important. Data backup is recording function to duplicate the necessary data and store it in a safe from both human and natural disasters. Then storing traffic data, another effective security provision is to monitor access to all of the data. Most computers can keep track of every change to every file. They can keep log of who accesses each file. Monitoring system and firewalls. Monitoring system is an activity after the computer can identify each user. User can control access to any piece of data, and firewall are essentially routers that examine each packet of network data passing through them and block certain types to limit the interaction of the network with the Internet. User identification is a process of identifying the user by asking to see identification. The most common method of identifying users to computers is with password .The last one is auditing system information is a process of identifying the user by asking to see identification. The most common method of identifying users to computers is with password [9].

TABLE II. KIND OF INFORMATION SYSTEM SECURITY MOST USED BY INSTITUTION

| Kind of Information System Security | Number/Units | Percentage |
|---|---|---|
| User Identification | 22 | 73 |
| Monitoring System | 26 | 80 |
| Data Backup: | 24 | 87 |
| Storing Traffic Data | 25 | 83 |
| Firewalls | 24 | 80 |
| Antivirus | 30 | 100 |
| Intrusion Detection System. | 27 | 90 |
| Auditing Information System | 20 | 67 |

Source: Result of Data

## IV. CONCLUSION

The conclusion of this study is that higher education institution as a non-profit organization is not immune from computer crime activities. Higher education institutions have implemented information systems security policy. Some of the policy declared officially in higher education institutions however many do not declare the policy. Application of UU ITE 11, 2008 have not been fully implemented.

UU ITE 11, 2008 as a public policy has been running in Indonesia however until now there is no implementation regulation thus the interpretation of the provisions in it to be varied in the community.

The lack pressure, coercion or penalties from government to the institutions that do not conduct to the maximum of information systems security

## V. SUGGESTION

Higher education institutions must be raise awareness the threat of computer crime. Required a deep understanding of the content of UU ITE 11, 2008 by each institution of higher education to apply information systems security.

The government should be issue government regulations to adjust the existing provisions in the Act ITE 11, 2008 in order not to be a debate in the society.

## REFERENCES


[1] Doney, Lloyd, “Nonprofits Aren’t Immune to Computer Crime”, Articles Nonprofit World, Vol.19, Number 2 March/April 2001 Odana Road Suite 1, Madison, USA p.33

[2] Icove, David., Seger, Karl., and VonStorch, William, Computer Crime, A Crimefighter's Handbook, O'Reilly & Associates, Inc. 103 Morris Street, Suite A Sebastopol, CA 95472. 1995, p.66

[3] Newton, Michael, *The Encyclopedia of Crime Scene Investigation*, Infobase Publishing, Inc. USA, 2008, p.121

[4] Laudon. C Kenneth, “ Management Information System”, Prentice Hall USA, Laudon, 2008, p.264

[5] Islamy , M. Irfan, “Principles of Nations Policy Formulation” (Prinsip-Prinsip Perumusan Kebijaksanaan Negara), Bumi Aksara, Jakarta, 2004 p.106.

[6] Nazir. Moh., “Research Method” (Metode Penelitian) : Ghalia Indonesia Jakarta, 1988, p:63

[7] Vacca, John R, “Computer and Information Security Handbook”, Morgan Kaufmann Publishers is an imprint of Elsevier. 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA, 2009, p:232

[8] Senn, James A, “Information Technology in Business, Principles, Practices, and Opportunities”, Prentice Hall International Inc, 1995, p.548.

[9] Post, Gerald V. and Anderson, David L. *Management Information System,* McGraw-Hill/Irwin USA 2006, pp 174-189