SUCCESS OF IMPLEMENTATION OF COMPUTER CRIME ACT (UU ITE NO.11 2008) (A Case Study in the Higher Education Institution in Indonesia)

Rizki Yudhi Dewantara
Student of MPA Double Degree Program at Faculty of Management Sciences
Prince of Songkla University, Thailand
and
Faculty of Administrative Science-University of Brawijaya, Indonesia

ABSTRACT

Computer crime rate grow rapidly along with the development of the digital world that has touched almost all aspects of human life. Institutions of higher education cannot be separated from the problem of computer crime activities. The paper analyses the implementation of Indonesia Computer Crime Act (UU ITE NO.11 2008) in the Higher Education Institution in Indonesia. It aims to investigate the level of computer crimes that occurred in the higher education institution environment and the act (UU ITE 11, 2008) successfully applied to prevent the crime that would arise. In this research, the analysis using Descriptive Statistics, Binary logistic regression. This paper also describes the success implementation of the Information System Security Policy (ISSP) as a computer crime prevention policy in higher education institution in Indonesia. In factor of act, clarity of objectives and purpose of the UU ITE 11, 2008 was low, the communication and socialization activities are still low to the society especially to the higher education institution, moreover the control process has been running on UU ITE 11, 2008, but at a low level.

Keywords: computer crime, computer crime act, public policy implementation

ABSTRAK

Kejahatan Komputer berkembang pesat sejalan dengan perkembangan dunia digital, pada institusi perguruan tinggi tidak dapat dipisahkan dari bagian kejahatan computer. Penelitian ini merupakan analisis kesuksesan penerapan undang-undang kejahatan komputer (UU ITE 11, 2008) di institusi perguruan tinggi di Indonesia. Penelitian ini bertujuan untuk mengetahui tingkat kejahatan komputer yang terjadi pada lingkungan institusi perguruan tinggi dan kesuksesan penerapan undang-undang kejahatan komputer untuk mencegah tindakan kejahatan komputer yang mungkin dapat terjadi maupun menangani kejahatan yang sedang terjadi. Berdasarkan tujuan penelitian, digunakan pendekatan quantitative dengan beberapa uji statistic antara lain analisis statistic deskriptif, dan regresi logostik binari. Hasil penelitian menjelaskan tingkat kesuksesan penerapan kebijakan keamanan sistem informasi sebagai tindakan pencegahan kejahatan sistem informasi di Institusi perguruan tinggi di Indonesia. Hasil penelitian menyatakan bahwa rendahnya faktor undang-undang, kejelasan isi dan tujuan dari kebijakan kemanan komputer di institusi perguruan tinggi mempengaruhi tingkat kesuksesan penerapan kebijakan kemanan sistem informasi, selanjutnya proses pengendalian telah berjalan pada UU ITE 11, 2008, namun pada skala yang rendah.

Kata Kunci: kejahatan komputer, undang-undang kejahatan komputer, implementasi kebijakan publik

INTRODUCTION

The more people who have to rely on computer systems, it has many advantages such as speed in the processing of mathematical calculation, accuracy in solving problems on the job, and computer systems are also able to minimize the quantity of work is high and reduces the number of errors that occur.

Misuse of computer technology is the impact of rapid technological development itself. Advances in technology such as the tools of information technology and communication technology raises new crime that has different characteristics from conventional crime. Apart from the positive side, the development of computers and the Internet also raises a lot of negative impact that crime has increased in the use of computer applications and crime over the Internet. Computer crime by using information technology developments have led to substantial losses. Information technology tools are promising computer speed and cost efficiencies that benefit the organization in line with it make it easier for criminals also launched a computer in a crime.

The purposes of computer crime are wide ranges of computer crimes are not boundaries by the age, sex, race, as long as the computers that have the potential to cause crime, then anyone can commit a crime. As an example, reported to the ACFE (Association of Certified Fraud Examiners) 755 of perpetrators were the resource persons and 25% were the resource to women. Most are first-time perpetrators, having no previous criminal record (Doney 2001). The motives of computer criminal might be various. Motivation ranges from money to fun, from economic gain to intellectual challenge, from revenge to "why not?" In some cases, there may be more than one motivational factor. (Icove, Seger and VonStorch 1995; 66). Computer crime also can occur in both agencies of government-owned or private.

In Indonesia, a number of laws protect against attacks on computers, misuse of passwords, electronic invasions of privacy, and other transgressions. Indonesia already possess a criminal record in the computer field since the beginning of 1980, attacks on bank computer system by employee occur in government owned bank, and another form of computer crime in recent years is the abuse on internet that is about piracy and theft through the internet site, 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 accident and in 2004 there were 1103 such cases. These cases are not much dealt with firmly by the authorities and not reported by the victims (www.tekno.kompas.com/read/2008/ 06/07/15301865).

There are several other positive laws that apply generally and may be charged for the perpetrators of computer crime, especially for cases that use computers as a means, such as:

a. Indonesian Criminal Code (Kitab Undang-Undang Hukum Pidana)
b. Law of Republic Indonesia No. 19 Year 2002 concerning Copyrights. (Undang-Undang No 19 Tahun 2002 tentang Hak Cipta)
c. Law of Republic Indonesia No. 36 Year 1999 concerning Telecommunication. (Undang-Undang No 36 Tahun 1999 tentang Telekomunikasi)

Indonesia Computer Crime Law has signed by the president on 25 March 2008, 10 approved the bill ITE fraction determined to be a Law. Furthermore, President Susilo Bambang Yudhoyono signed script UU ITE became the Law of the Republic of Indonesia Number 11 Year 2008 on Information and Electronic Transaction, and published in State Gazette Number 58 Year 2008 and Supplement. Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2008 also called UU-ITE No. 11 Year 2008 is the main piece of legislation that governs most common computer crimes, although many other laws may be used to prosecute different types of computer crime.

The role of information and communication technology in education is also very important, especially in terms of supporting the teaching-learning process and the efficiency of academic and administrative jobs. Higher education institution in Indonesia are categorized as academic education and vocational or higher in science, technology, and/or art. Higher Education as one of the educational institutions, should be able to utilize information and communication technology in support of various activities not only in academics but also for society. The application of information and communication technologies in higher education activities will

provide a very positive impact and is expected to provide an efficient and productive results in academic and administrative fields. Implementation and adaptation of information and communication technologies in higher education, is also expected to be competitive in the arena of higher education at the national and even international level. Use and utilization of information technology (IT) in higher education is very high, it can be proved by statements from a number of universities, which states that already utilize IT facilities through the provision of Information and Communication Technology (ICT). Interaction among other academics member such as professors and students not only done through face to face relationship but can also be done by using information technology media such as the Internet, e-mail, teleconferencing, social media, Internet-based applications and mobile based etc.

In higher education institutions, computer crime activities are also very common. Crimes such as unauthorized access, data theft, pornography and sexual abuse, and also control unauthorized sites owned by other institutions, carried out in higher education institutions. Higher education institutions are too risky from the threat of computer crime both inside and outside of the institution. Institutions of higher education have strategic data stored in the data storage facility, thus attract to anyone who wants to try to do the crime of the computer systems on campus with a variety of motives. Computer crime cases that occurred in higher education institutions, for example such as steal or modify data that is confidential, changing the status of student member, manipulate the test scores, and much more related to the activities in educational institutions.

These data could be misused for personal benefit or group of people. Another case occurs for example, destroy the important data that stored in data center by break through the security information systems and spread the virus so that the user cannot access the data. Several prevention actions are needed to protect the information security on higher education institution, such as computer crime act and security policy.

Application of the law, especially for computer crime is very important. The law is a manifestation of public policy created by the government to achieve certain goals, while policy implementation is the process of implementation of the policy. The government should provide a way to implement the policy so that they can have an impact or influence on something. The focus of policy implementation is an event or events that arise after the policy that led to the need for guidelines for the implementation of state policies that include efforts to bring results or real impact on society after the policy is implemented. These guidelines can be administrative activities and to organize the implementation of policies.

THEORITICAL BACKGROUND AND HYPOTHESIS

Policy can be defined as the programmatic activities formulated in response to an authoritative decision (Matland 154, 1995). Ingram and Schenieder (1990) note several plausible definitions of successful implementation. Among these are: agencies comply with directives of the statutes; agencies are held accountable for reaching specific indicators of success; goals of the statue are achieved; local goals are achieved or there is an improvement in the political climate around the program (Matland 1995;154).

Based on that reason, it is necessary to implement the computer crime act (UU ITE No.11, 2008) in higher education organizations. Some of the articles that regulate the University or institution of higher education is mentioned as follows:

1. Article 1 section 5, which mention University or Higher Education Institution categorized as a Provider of Electronic system and strategic database.
2. Article 40 section 2, mention about Higher Education Institution categorized as a public service institution should be safe from thread of any crime in information system.
3. Article 52 sections 2, which mentions Higher Education Institution as an agent which have strategic computer or electrical system as well as electronic information or strategic data.

Indonesia computer crime act (UU ITE 11, 2008) has applied in Indonesia, after it implemented many questions and cases arise whether this policy has actually implemented on every layer of society or whether it has implemented effectively. Some factors influence the successful implementation of this

computer crime act, the society often look at that success can be measured by the extent the of the effectiveness of the policy implementation, or the goals of the policy should be achieved. This study was conducted to identify and study the factors affecting the success of Computer Crime Act UU ITE No.11 2008 implementation, which applied at higher education institutions as a public-sector institution in Indonesia. Successful implementation of this law will be seen from two factors which are the policy factors and organizational factors. Each factor is based on theoretical studies relating to the successful implementation of policies on the organization. Furthermore, the result of this study will inform the factors that most influence on successful implementation of the Computer Crime Act apply to higher education organizations. The results of this study as a guideline for the management and executive staff on department of information technology, especially in college, and to identify factors that need to be improved or developed.

Hypothesis

Based on the proposed conceptual framework, four hypotheses were developed and analyzed.

1) The degree of implementing information system security policy in universities in Indonesia is high.
2) Perception of heads of IT department about the computer crime act (UU ITE 11, 2008) in universities in Indonesia is highly positive.
3) Perception of heads of IT department about the organizational disposition in universities in Indonesia is highly positive.
4) Only the policy factor (Computer Crime Act – UU ITE 11, 2008) affect positively on implementation of information system security policy in universities in Indonesia.

Objective of the Research

1. To evaluate the degree of success policy implementation computer crime act (UU ITE No.11, 2008) applied at Higher Institution of Education in Indonesia.
2. To investigate the factors affecting the success of Computer Crime Act (UU ITE No.11 2008) In the Higher Institution of Education in Indonesia.

Benefit of the Research

1. This research value will enrich the substantive scope and method of public administration especially related to The Public Policy Implementation.
2. Findings obtained from this research will share valuable information to Higher Education Institution and Government of Indonesia in order to improve the effectiveness of Computer Crime Act implementation.

Scope of The Research

The focus of this research is the implementation of the act, which is Computer Crime Act (UU ITE NO.11 2008) as the product of policies generated by the government in terms of computer crime that occurred in higher education or university institution in Indonesia. This research aims to study:

1. Degree of successful implementation of Act. UU ITE 11, 2008 in higher education institution in Indonesia.
2. Factors of affecting the successful implementation of Act. UU ITE 11, 2008 in higher education institution in Indonesia.

RESEARCH METHOD

This Study will use survey research, which is research conducted to obtain the facts about the conditions of IT management from the existing symptoms and seeking factual information on higher eduction institution. Site to research is Java Island is one part of five big islands in Indonesia, it consists of six provinces, which are Banten, Jakarta, West Java, Central Java, Yogyakarta and East Java. Java Province is still the most densely populated areas in Indonesia, which includes a half (57.5%), Indonesia's population. (BKKBN, www.bkkbn.go.id). Based on the census in 2010 showed the total population in Indonesia increased to 237.641.326 people, with high population growth rate is at 1.49 percent. With these population data, the number of higher education institution are also widely available on the island of Java.

In this study the population is the head of department/staff of Information Technology (IT) Department in higher education institution that is located on the island of Java. Reason determining the study population on the island of Java is the highest number of higher

education institution in Indonesia is concentrated in Java Island (see table1).

Table 1: Number of Higher Education Institution

Higher Education Institution	Number/ Units	Percent
Public	83	3
Private	2.987	97
Total	**3.070**	**100**

Source: APTIKOM 2010

According to the Indonesia General Directorate of Higher Education (DIKTI, 2010 http://dp2m.dikti.go.id), the number of Institution in 2010 are 3070 institution. The Classification of higher education institutions shown in table 2.

Table 2: Number of Higher Education Institution by Classification

Classification of Higher Education Institution	Number/Units
University	465
Higher School Institution	1.345
Institute	55
Academy	1.037
Polytechnic	168

Source: APTIKOM 2010

The total number of higher education institution in Island of Java described in table 3.

Table 3: Total number of Higher Education Institution in Java Island

Province	Total
Banten	99
DKI Jakarta	336
Jawa Barat	399
Jawa Tengah	253
DI Yogyakarta	126
JawaTimur	341
Total	**1554**

Source: http://evaluasi.dikti.go.id/database/pt

Data Collection Method and Data Analysis

The collection of data used in this study is using a structured questionnaire which is the method gave a statement in response to the questionnaire. The questionnaire comprised of several chapters that explanation of research purposes and list of the question. In the early chapters of the questionnaire the researcher identifies the purpose of the survey respondents purpose is to determine the response of IT staff who are in the institution of higher education. The next chapter contains a list of questions related to computer security policies in campus. Once filled out by respondents, researchers can directly collect answers to questionnaires for data processing.

In this study, based on the respondent's perceptions, the success of Information System Security Policy implementation in the higher education institution of Indonesia was the dependent variable. There are two independent variables in this study, as shown below. Member of ICT Department in higher education institution would answer the questionnaires based on these two independent variables according to their perceptions. Independent variable consists of two factors which are: Law Factors (The Act and Regulation) consist of: Objective and the purpose of the act, Clarity of the Act, Control process, and next factors is Factors of Organization which consist of: Leadership, Human Resources, Organizational structure, Financial and Physical resources.

In this study, types of statistics are used in quantitative research, which are: Descriptive Statistics Analysis, Binary logistic regression and the model used in the logistic regression was:

$$Ln\frac{F}{1-F} = \alpha + \beta 1X1 + \beta 2\,X2 + e$$

Where:

$Ln\frac{F}{1-F}$	=	The tendency of the application ISSP (dummy, 1 = apply the ISSP, 0 = do not implement ISSP
α	=	Constanta
$X1$	=	Factor of Policy / Act
$X2$	=	Factor of Organization
$\beta 1 \beta 2$	=	Regression coefficient for each independent variable
e	=	Error

RESULT AND DISCUSSION

The main objectives of this study were to: 1) evaluate the degree of implementation

Information System Security Policy in higher education institutions in Indonesia. 2) To investigate the factors affecting implementation of Information System Security Policy in higher education institutions in Indonesia. Data collection in this research was located higher education institution in Indonesia and based on Java Island. Reason determining the study population on the island of Java is the highest number of higher education institution in Indonesia concentrated in Java Island.

In this study the population is the head of department/staff of Information Technology department in higher education institution. Amount 316 higher education institution observed in this study through the period of May 2012 and October 2012. Data was analyzed using binary logistic regression (logit) multiple regression technique.

The Result revealed as follows.

1) Number of the higher education institutions were implement the IS Security Policy as much as 66%, but only 46% were declared the IS Security Policy. The facts convince that larger than member of the higher education institutions implementing IS security policy as one of the computer crime prevention, although from total the institutions that conduct information system security policy is not totally followed by the declaration of policy in the institution.
2) Two preparation activities securing information system, which is the focus of information system security policy higher education institutions against computer crime, which are Administrative preparation and technical preparation. Administrative preparation focused on such documentation and procedural steps of policies and guidance, then Technical Controls focused on use of software and hardware resources to control access to information and computing systems and other activities in practice. Based on the survey results determined that technical preparations are better than the application of administrative preparation, where the percentage of implementation of technical activities are higher than the application of administrative activities. As shown in small number of special handling computer crime unit and the provision of documents on ISSP, however for technical activities such as data backup to Data Backup Log has a high number of applications to higher education institutions. Only activities that use specialized software and hardware that IDS and the Information Systems Audit has a low adoption in higher education institutions. Meanwhile a low percentage is also found in the implementation of training on handling computer crime for staff and students. As shown in small number of special handling computer crime unit and the provision of documents on ISSP, however for technical activities such as data backup to Data Backup Log has a high number of applications to higher education institutions. Such activities that use special software also hardware that IDS and the Information Systems Audit has a low adoption in higher education institutions. Meanwhile a low percentage is also found in the implementation of training on handling computer crime for staff and students.
3) Two factors of study are factor of act and factor of organization, the result of descriptive statistic was; In factor of act, clarity of objectives and purpose of the UU ITE 11, 2008 was low, the communication and socialization activities are still low to the society especially to the higher education institution, moreover the control process has been running on UU ITE 11, 2008, but at a low level. Then at factor of organization, the higher education institution executive leadership style sufficient to support the application of computer crime act moreover need better awareness of the issues of computer crime, human resources is able to support the implementation of computer crime act, organizational structure of higher education institutions can be strength for the application of computer crime Act, furthermore the institution have a strong resource of funding and physical, as well as procedures to use them, nevertheless programs of information technology, including information systems security is not the first priority for higher education institutions.
4) From the results of processing the data using logistic regression method known that, the coefficient of determination seen from Nagelkerke R Square are 0793 (79.3%). It means the independent variable (policy factors and organizational factors)

could explain the dependent variable (Implementation of Information System Security Policy) by 79%, while the rest can be explained by other factors outside of the observed variables. The study reveals that Act exhibit a direct and the positive relationship with the success of ISSP implementation, with a Sig value X_1 of 0.00 ($P<0.05$). Another independent factor-organization, which can be defined as leadership, human resources, organizational structure, fund and physical resources, has a direct and positive relationship with the success of ISSP implementation in higher education institution, Sig value X_2 of 0.00 ($P<0.05$).

From the findings of study, it can be concluded that in order to implement ISSP in higher education institution successfully, the major concern should be placed on the factors of Act, and factors of organization.

CONCLUSION AND RECOMMENDATION

Conclusion

It can be concluded that in order to implement ISSP in higher education institution successfully, the major concern should be placed on the factors of law condition, and factors of organization. The better the support of these factors, the higher the success of ISSP implementation will be. This study related to previous study by Percival in 2004 that implementation of act regarding to drug policy in California's local government. The implementation requires cooperation between county and state institution, including local government and community. Furthermore, the study also related to previous research by Phaopeng (2010) that the success of ICT policy implementation in education is determined by the policy conditions, the characteristics of school directors, and the characteristics of teachers and students. For the organizational factor the result of research relate to study by Mitchell (2010) that the organizational factor as a one of key categories of success in implementation program. Some of the key organization factors that have attracted attention from implementation researchers include leadership and organization structure. Based on the result presented in this thesis, a contribution to evaluation of improved success implementation of UU ITE 11, 2008 in Indonesia higher education institution was made. Low percentage appears on the availability of a special unit or workgroup for information system security. Concern of leaders to the security of information systems by organizing a special unit or workgroup security information system is needed in higher education institutions. Higher education institution also has a low percentage of administrative preparation, especially the provision of documents relating to the ISSP and prevention of computer crime. Procurement documents to all users of IT can enhance the user's knowledge of the security of information systems.

Recommendation to Higher Education Institution

1) Higher education institution needs to implement the technical preparation activities according to Indonesia Information Security Standards (ISO) ISO/IEC 27001: 2009.
2) More support from executive specially in increasing knowledge of information system security and computer crime also more attention to ICT priority regarding funding and physical resources will strengthen the success of computer crime act implementation.

Recommendation to Government

1) Issuing government regulations to simplify the understanding and implementation of the UU ITE 11, 2008 by the institution.
2) Improve socialization of information system security to institutions of higher education, such as the application of ISSP which is appropriate to Indonesia safety standards (SNI) ISO / IEC 27001:2009, also providing technical guidance information system security policy implementation.

REFERENCES

Dye. Thomas R, Understanding Publik Policy (tenth edition). New Jersey: Prentice Hall, 2002.

Faisal. S. "Social Research Format" (Format Penelitian Sosial) : Rajawali Press, Jakarta, 1990.

Islamy , M. Irfan, "Principles of Nations Policy Formulation" (Prinsip-Prinsip Perumusan Kebijaksanaan Negara), Bumi Aksara, Jakarta, 2004.

Laudon. C Kenneth, " Management Information System" 7th Edition, Prentice Hall USA, 2002.

Nazir. Moh., "Research Method" (Metode Penelitian) : Ghalia Indonesia Jakarta, 1988.

Potter, Richard E., Rainer Jr, Kelly R., Turban Efraim., "Introduction to Information Technology", Wailey and Sons Inc, USA, 2005.

Rahardjo. Budi, Ir. M.Sc, Ph.D, "Understanding Information Technology" (Memahami Teknologi Informasi) : Elex Media Komputindo, Jakarta, 2002.

Rosenbloom, David H., and Kravchuk Robert S., "Public Administration, Understanding Management, Politics, and Law in The Publik Sector", McGraw-Hill, USA, 2005.

Ross J. Anderson, Frank Stajano, Jong-Hyeon Lee, "Security Policies". Advances in Computers (AC) 55:185-235, 2001.

Salomon, David, "Elements of Computer Security", Springer-Verlag Limited, London, 2010.

Senn, James A, "Information Technology in Business, Principles, Practices, and Opportunities", Prentice Hall International Inc, 1995.

Sieber U. Prof. Dr. "Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society", article in the German language published in Komputer und Recht (CR) 1995, pp. 100 et seq. http://www.uplink.com.au/lawlibrary/ accessed on December 17, 2010

Sugiyono, "Research Method for Administration and Management (Metode Penelitian Administrasi dan Manajemen), Bandung, Alfabeta 2007.

Sundt, Chris, "Information Security and The Law", Information Security Technical Report 11 (2006) 2-9, Elsevier Science Limited.

Tipton, Harold F., and Krause Micki, "Information Security Management Handbook" Fifth Edition, Volume 2, Auerbach Publikations, A Crc Press Company Boca Raton London New York Washington, D.C. , 2003

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.

Walton, Richard, "The Computer Misuse Act", Information Security Technical report 11, Elsevier Ltd, 2006.