The Threat Level

by Dian Indri P

Submission date: 15-Nov-2017 09:45AM (UTC+0700)
Submission ID: 880069251
File name: The_Threat_Level.pdf (209.08K)
Word count: 3657
Character count: 19455

International Journal of Computer Networks and Communications Security

VOL. 2, NO. 5, MAY 2014, 173–178
Available online at: www.ijcncs.org
ISSN 2308-9830

The Threat Level Tolerance in the Company of Accounting Information System

Dian Indri Purnamasari[1]

[1] Pembangunan Nasional University "Veteran" Yogyakarta-Indonesia

E-mail: [1]*indri_mtc@yahoo.com*

ABSTRACT

Accounting information system developments that provide benefits in many organizations it also has risks that are not light. How can an organization tolerate the possibility of a threat in the accounting information system will be different with other organizations. This study wanted to know whether there 12 differences in levels of tolerance to the threat of companies in the accounting information system. With a sample of all companies listing on the Indonesia Stock Exchange (IDX) and the rate of return of 18.8% of respondents, this study provides a statistical conclusion that there is no difference in the level of tolerance to the threat of accounting information system among companies listing on the IDX. This is because companies are listing on the IDX is a company that is ready for the public so that they also prepare all the things associated with information systems, including accounting information system and the maximum fine.

Keywords: *Accounting, System, Information, Threat, Tolerance.*

1 INTRODUCTION

Information system has advanced rapidly with the development of computer-based technology. In the field of accounting, the development has resulted in Accounting Information Systems (AIS). Today, it is hardly possible for companies (organizations) not to adopt computerized AIS. There are a lot of things to do with the computerized AIS, among others, organizing an increasingly globalized activity at the international as well as local level. Activities in many organizations were made easier with the presence of computerized AIS. For example, organizations were no longer need to perform data transmission via postal service that takes much longer time, but over the internet protocol. In fact, it is possible for them to exchange information on accounting data with the help of computers and the Internet.

Development of the AIS, which provides many benefits and advantages to organizations, brings also no small risk, which is a threat contained in the input, process, or output. Any mistake in accounting data entry, whether committed intentionally or not, can have significant impact on the operating activit 2 of the organization, and this is one of the threats to the system. Accounting data loss due to a defect in storage system and to the error in AIS design might also jeopardize organizational activities. Any development of AIS has positive and negative effects, and it is no secret to many organizations that develop and use the system. The question that subsequently arises is how much effort an organization should expend on anticipating the threats. Although much has been done by accountants in designing AIS to reduce the threat in it, the demand for the use of this system continues to increase [1]. How much effort expended to anticipate the threat is reflected in the organizational tolerance for the possible threats in the AIS.

How one organization tolerates the possible threat in the AIS 2 be different to that of another. Perhaps, some organizations are so strict in designing AIS that they will not tolerate any threat or, in other words, they will directly address the

[1] This research funded by the Directorate General of Higher Education, Ministry of National Education. Research Lecturer in the program Youth and Women's Studies, 2007 and presented on The 2nd International Conference on Business and Banking. Bali, Indonesia, 2012 and has been improved as proposed during the discussions.

emerging threats, so it is not possible for them to reappear. In contrast, some other organizations might still tolerate such a threat so it is possible that the same threats will appear several times within a certain period of time.

Musa [2] in his study, which used a sample of all organizations in Saudi Arabia, concluded that there was no significant difference between the various organizations in that country in terms of tolerance for threats to the computerized AIS. Some types of threats are often experienced by many companies, which indicate a similar degree of tolerance for the threat in AIS. Among these threats are the mistakes made by employees in entering data, and it is very tolerable because it is humane. The author in this study intends to determine whether the organizations in Indonesia have the same tolerance level for threat in the AIS.

Based on the background of the research mentioned above, the problem formulation will be is there any differences in the degree of tolerance to the threats in AIS among companies listed at IDX? The current study aims to provide empirical evidence of whether there are differences in the level of tolerance to the threats in among all companies enlisted at IDX. It is the author's hope that this research will be beneficial to the development of AIS, especially for companies that went public, in tolerating threats in AIS.

2 LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Level according to Sihwahjoeni [3] the processes of selection, grouping, and interpreting. Desriani [4] stated that level is the information extraction process. In Encyclopedia of Psychology it is described that level shows the sensory experience in the form of information about people, objects, and events, as well as psychological processes to refine the information. Kamus Besar Bahasa Indonesia defines level as direct response (acceptance) to something or a process through which an individual knows something through his/her senses. Eko defines that level represents an experience about objects, events, or relationships acquired by inferring information and interpreting messages. Level is a process by which a person interprets stimuli he/she has received and also a process by which a person organizes his or her thoughts by interpreting or experiencing them, and by processing the signs or anything happens around him/her. Thus, level can be interpreted as cognitive processes experienced by every person in understanding any information about environment through the five senses [3].

However, because the level of objects or events depends on a framework of space and time [5], it will also be very subjective and situational in nature. In addition to being implicitly stated in the definition above, this argument is also consistent with that proposed by Eko [5] that level is determined by personal and situational factors, which referred to as functional and structural factors. The functional factors are derived from needs, past experiences, and other things included in what is referred to as personal factors. Therefore, what determines the level is not the type or form of stimuli, but the characteristics of person who respond to them. Structural factors derived solely from the physical and neurological effects they cause on the nervous system of individuals. Therefore, according to Eko [5] based on Gestalt theory, if we intend to improve something then we improve it as a whole. To put it differently, if we want to understand an event we can not examine the facts separately, but we must look at the overall relationship.

Tolerance is how events or threats to AIS may occur within a certain period. If the threats to AIS are frequently occurred, then the tolerance is so high that they were allowed to occur repeatedly. If the company does not tolerate the threats to AIS, it will handle them as they emerged and anticipated to prevent them from happening in the future. AIS designs were made to realize an effective and efficient system of internal control, which, among others, is directed to put off the threat to SIA within the organization.

Loch [6] conducted a test at the managerial level of the Management Information Systems (MIS) to determine the security level of the microcomputer, mainframe computer and network environment. In their research, Loch [6] developed the threat level to the MIS into 12 levels, and respondents were asked to rank the highest threat (top rank). Respondents in the study stated that the threat of natural disasters (e.g. the threat of hackers and ineffective control) and errors by employees are the two things ranked at the top of their selection.

Davis [7] replicates the study by Loch [6] with the respondents that were members of the Information Systems Audit and Control Association (ISACA) and Certified Public Accountants (AICPA). He concluded that auditors with different AIS computerized environment will have different levels of tolerance of threats to AIS. Computerized systems associated with parties outside the company will have a higher risk level than a system that is only related to the environment within the company.

Ryan [8] study categorized threats to AIS into 15 instruments, and distributing questionnaires to information systems technicians of medium and large companies that are organizing a conference. The results showed that different companies have different tolerance levels against threats to AIS, although the threat in the form of errors by the employee still occupying the highest ranking of each respondent. Instrument in this study still has many shortcomings, according to some opinions of other investigators, and thereby need to be modified and refined in the future.

Henry [9] attempted to identify to what extent the companies provide the level of tolerance to AIS threats which is reflected by the level of security in entering the system. The study concluded that 80% of companies have already backed up their information systems, 75% have been securing their system by creating a password, while the rest just do security to address the possibility of computer viruses. This shows that in fact many companies have different tolerance levels against threats to AIS.

Musa [1] classifies the threats to AIS into 19 instruments and applies them to the banking companies in Egypt. Instrument developed in this study adopted and perfected that of previous research mentioned above and using 5-point scale on the frequency of threat in the companies. The results showed that there was no difference in levels of tolerance to the AIS threats among the types of different banks.

Musa [2] developed his previous study using a sample of all organizations in Saudi Arabia. He concluded that there was no significant difference between different organizations in Saudi Arabia in terms of tolerance to the threats that occur in computerized AIS. Some types of threats that are often experienced by many companies indicate a similar tolerance to the threat of the AIS, such as the employee made mistakes in entering the data, which is a very tolerable and humane.

This study replicated that of Musa [2] because, as far as the author concerned, similar studies have not been conducted in Indonesia by using a sample of all ISX-listed companies. Different types of companies will have different tolerance levels against threats in the AIS, for example: Banks will have a lower tolerance level compared to other types of companies as banks or other financial institutions have a greater risk in terms of their customer finance than real estate companies

Based on the above findings, the author formulated the following hypothesis:

Ha: There are differences in the level of tolerance to AIS threats among IDX-listed companies.

3 RESEARCH METHOD

3.1 Determination of Sample

The sample in this study is the population of all IDX-listed companies. The selected respondents were the companies' internal auditors because they are able to design the AIS and to detect any weaknesses in it. The choice of companies enlisted at IDX is because they are public companies that require greater control in terms of AIS and should not tolerate any threat in it. A question to be answered in this study is whether in fact this is so. The data was collected through mail surveys.

3.2 Identification and Measurement of Variables

Tolerance for threat to AIS was measured using instruments developed by Musa [2] which comprised 19 items of question about the possible frequency of the occurrence of the threat in AIS. Respondents were asked to answer how often the threat is happening within the company in a 5-point scale (had never, almost never, sometimes, often and always).

3.3 Validity and Reliability Testing

The research data will not be useful if the instrument used to collect them do not have the reliability and validity [10]. Reliability testing is intended to determine the extent to which the measurement is consistent. An instrument is reliable if it has a Cronbach alpha greater than 0.6 [11]. Validity testing was to evaluate how well the measuring instrument measures what it is supposed to measure. A variable is valid if it has factor loading larger than 0.4 and eigenvalue greater than 1 [11].

3.4 Pilot Test

Before the questionnaire is given to the actual respondents, the author conducted a pilot test to determine the validity and reliability of the instrument and to avoid questions that are less obvious as well as to determine the time required to complete the questionnaire. The pilot test was conducted with 30 respondents who work as internal auditor in company and the results showed that all the research instruments used are valid and reliable.

3.5 Nonresponse Bias Test

The test of nonresponse bias was conducted to investigate whether there was a significant different in the characteristics of the sample of the respondents who responded and did not respond. They were divided in to two, which are the respondents who came early and represented those responding and the respondents who came late and represented those not responding and then t-test was conducted.

3.6 Hypothesis Test

The hypothesis test was conducted using One Way ANOVA.

4 DATA ANALYSIS AND DISCUSSION

4.1 Data Description

The following table illustrates the process of distributing questionnaires to obtain data and their rate of return.

Table. 1. Questionnaire Response Rate

Total questionnaire distributed	= 339
Returned and analyzed	= 64
Response rate	18,8%

Total of 339 questionnaires were distributed to internal auditors in IDX-listed companies, and the number returned for analysis amount to 64 questionnaires. The response rate is quite good because in general the response rate in Indonesia is in the range of 10%, whereas in the study it reached 18.8%.

Table. 2. Data on Companies Returning Questionnaire

Company	Amount
Farming and Fishing	3
Mining	2
Manufacture	33
Transportation	4
Telecomunication	2
Retails	6
Banking and Financial Service	10
Others	4
Total	64

The above table shows that the companies returning questionnaire are mostly of manufacture (51%) and banking (15%). This was so because the composition of manufacturing and banking companies enlisted at IDX outnumbered other type of companies, i.e. 43% and 30% for manufacturing companies and banking and financial non-banking companies, respectively.

4.2 Nonresponse Bias Test

The results showed that there was not any significant difference in the respondents who did not respond or submit them. Therefore, there was not any problem of response bias.

4.3 Validity and Reliability Testing

The result of validity and reliability testing show that all of accounting information system variable are reliable with 19 questioners and the cronbach alpha 0,910 and valid use pearson correlation analysis.

4.4 Descriptive Statistics

Var	N	Min	Max	Mean	Stándar Deviation
SIA	64	2,95	4,84	3,96	0,49

4.5 Examining Anova Assumptions

Hypothesis testing using the ANOVA requires several assumptions tests that must be met in order that the results of ANOVA can be used to make a conclusion about this study. Anova assumptions to be fulfilled are [11]:

a. Homogeneity of variance

Dependent variable in this study should have the same variance in each category of independent variables. Levene test results used to see the homogeneity of variance with a significance level > 0.05 concluded that the group has the same variant or, in other words, the assumption of equal variance was met.

b. Random sampling

For the purpose of significance testing using ANOVA, sampling within each group was taken randomly and the sample taken in this study is the entire population. Anova remain robust even if the sampling was not random, and subsequent analysis can be performed.

c. Multivariate normality

The variables must be normally distributed, but Anova remain robust even if it was not normally

distributed, and subsequent analysis can be performed. The variables in this study were normally distributed so that the normality assumption fulfilled.

Assumption of ANOVA test showed that all assumptions are met so that the hypothesis testing using ANOVA can be continued in subsequent analysis.

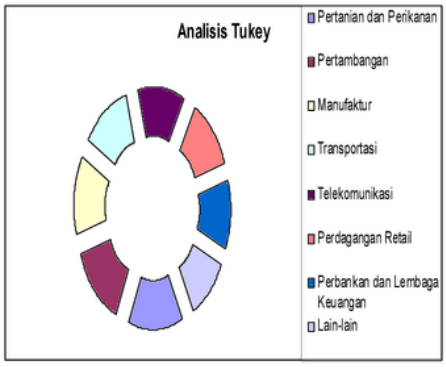
4.6 Hypothesis Testing

Variable	F test	Sig
SIA	1,657	0,139

The table shows the statistical significance of 0.05, which means there is no difference in the level of tolerance for the threat of AIS among the companies enlisted in IDX. Test results show that Ha is not supported. It is not supported because the IDX-listed companies were ready for the public so that they also prepare all the things related to the information systems, including AIS, and in maximum effort. Reasonably good and tightly enforced regulation and supervision from the various parties associated with the procedures and processes even when they were public companies (e.g. Bapepam) has contributed a great deal to make these companies a lot concerned about the development of company information systems. This has made these companies minimize the risk or threat in the AIS, and they no longer give a lot of tolerance against possible threats in the AIS, such as providing passwords to other parties by the employee. They already have a good control system for AIS, so there is no difference in the level of tolerance for threat in AIS among IDX listed companies, or in other words they have the same tolerance level for threat to AIS because they realize the importance of security in information systems, including AIS.

Table. 5. Tukey Analysis

Company	Amount	Average
Farming and Fishing	3	4,43
Mining	2	4,39
Manufacture	33	4,09
Transportation	4	3,98
Telecomunication	2	3,81
Retails	6	3,73
Banking and Financial	10	3,69
Service	4	3,34
Others		
Significance		0,054



The table above shows the average value of the tolerance level of each type of companies for the AIS threat. Significance level of 0.054 showed that the average level of tolerance of each type of companies for AIS thrats did not differ statistically with a significance level of 5%. The results support the decision that there was no difference in the level of tolerance for AIS threat among IDX-listed companies.

5 CONCLUSION, IMPLICATION, SUGGESTIONS, AND LIMITATIONS

5.1 Conclusion

This study concluded that among 18.8% IDX-listed companies there are statistically no difference in the level of tolerance for threat to AIS. This is because they are the companies that are ready for the public so that they also prepare all the things related to information systems, including AIS with both maximum and reasonably good effort. The companies enlisted in IDX have gone through several stages of the process of fulfilling the requirements made under the supervision of many external parties in IDX so they have the same rules for IDX listing. Similarity of the rules and procedures makes the levels of safety and tolerance for threats in AIS has no difference between them.

5.2 Research Contribution

The results of this study contribute to the development of AIS in the form of finding that firms with a lot of supervision in the form of regulation from various parties appeared to have the same AIS development, especially their perception of threat to AIS. It certainly would distinguish them from other companies that have no regulation or supervision from various external parties.

5.3 Limitation and Suggestion

This study has limitation in its sample, i.e. the companies enlisted in IDX with less than moderate response rate of 18.8%. This gives a great opportunity for future research to expand the study population to all companies in Indonesia and compares the various possible types or structure of corporate ownership.

6 REFERENCES

[1] Musa, Abu, Ahmad A., 2001, Evaluation The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry, PhD. Thesis, Aberdeen University, UK

[2] _____, 2004, Exploring The Perceived Threats of Computerized Accounting Information Systems in Emerging Countries: An Empirical Study on Saudi Organizations, The 7th European Conference on Accounting Information Systems, 30th-31st March 2004, Prague, Czech Republic

[3] Sihwahjoeni, M. Gudono, Tingkat Akuntan Terhadap Kode Etik Akuntan, Jurnal Riset Akuntansi Indonesia, Volume 3, No. 2, Juli 2000.

[4] Desriani, Rahmi, Tingkat Akuntan Publik Terhadap Kode Etik Akuntan Indonesia, Thesis S-2, Program Pasca Sarjana, Universitas Gajah Mada, 1993.

[5] Eko Prasetyo, Januar, Tingkat Perusahaan Asing Dan Perusahaan Dalam Negeri Yang Tidak Go Public Terhadap Kebutuhan Jasa Akuntan Publik, JAAI Volume 5 No. 1, Juni 2001.

[6] Loch, Karen D., Houston H. Carr and Merril E. Warkentin, 1992, Threats to Information Systems: Today's Reality, Yesterday's Understanding, MIS Quarterly, June, pp. 173-186

[7] Davis, Charles E, 1996, Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs, IS Audit & Control Journal, Vol. 3, pp. 38-41

[8] Ryan, S.D. and B. Bordoloi, 1997, Evaluating Security Threats in Mainframe and Client/Server Environmets, Information & Management, Vol. 32, Iss. 3, pp. 137-142

[9] Henry, Laurie, 1997, A Study of The Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia, The Mid-Atlantic Journal of Business, Vol. 33, Iss. 63, pp. 171-189

[10] Cooper, Donald dan Pamela S. Schindler, 2001, Business Research Methods,7th edition, McGraw Hill, Singapore

[11] Hair, Joseph, Rolph Anderson, Ronald Tatham dan William Black, 1998, Multivariate Data Analysis,5th edition, Prentice Hall International Inc, New Jersey

The Threat Level

ORIGINALITY REPORT

11%	8%	2%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.researchgate.net Internet Source	3%
2	Submitted to Hofstra University Student Paper	2%
3	Submitted to UI, Springfield Student Paper	2%
4	connection.ebscohost.com Internet Source	2%
5	faculty.kfupm.edu.sa Internet Source	1%
6	docplayer.net Internet Source	1%
7	Submitted to University of Ulster Student Paper	<1%
8	Submitted to Pasundan University Student Paper	<1%
9	documents.mx Internet Source	<1%

10	kpaj.or.kr Internet Source	<1%
11	bura.brunel.ac.uk Internet Source	<1%
12	informationstudies.net Internet Source	<1%

Exclude quotes	Off	Exclude matches	< 5 words
Exclude bibliography	On		