Information Technology Risk Assessment: Octave-S Approach

Bambang Gunawan, Alumni, Binus University,
Merry, Alumni, Binus University,
Nelly, Faculty Member, Binus University

Abstract - Purpose of the research is to identify the risk of IT in the company, to assess all the risk, and take security actions to solve the problem. Research methods used are data collection method and analysis method. Data collection is conducted with literature review and field studies by interview and observation. Analysis is conducted using Operationally Critical Threat, Asset, and Vulnerability (OCTAVE)-S method. The expected result is the risk identification in IT of the company.

Index Terms - IT, Risk Assessment, Octave-S

1. Introduction

Nowadays in business, the average of business entity implements the IT into their business process. IT becomes a base necessary for the company to survive in the business competitive. Many companies change their system into a computerized system. Computerized system will many benefit for the company such an efficiency of human resources, time and budget, and validity in company performance and also can help the management to take a decision.

According to Moteff [5], risk assessment will involve the integration of threat, vulnerability, consequence of information, and decide how the strategy to reduce the risk happened and it also inform the cost-effective allocation of resources to reduce the risk. There's some ways to reduce the risk happened and each ways give the potential countermeasures that may exist for particular assets, the analyst should do the feasibility of the countermeasures. According to Labriola [4], risk assessment can impact the surrounding structures were listed and assessed according to their potential likelihood and consequences by analyzed, elimination measures and re-calculate the measured being adopted.

This research will take place in GST, Ltd. This company focuses in construction and doing some material market like a techniques machines and building material. There are many competitors in this business type and IT becomes a necessary thing to improve the process.

2. Research Method

Research Method used in this research used a qualitative approach where the research will take a place in one of construction in Indonesia. Research Method will be divided into 2 types, data collection and analysis method. Data collection is conducted by using book studies and field studies. Book studies by collect the information from the book and journal. Field studies are conducted using interviews, observations, and questionnaire. Then for analysis method was done by assess the risk of IT in the company using a Octave-S approach and this assessment goes to the employees in the company which have more than 100 persons.

3. Literature Review

According to World Bank Group [7], Risk assessment will combines the exposure and the response to calculate the risk estimates such a number of people, predicted to experience and risk described uncertainties in the calculation and provides other information to help the analysis result. An effective risk assessment must have a well defined scope depends on the purpose of analysis, and the purpose have to identify the most healthy point from the people affected. Analysts have to choose the type of risk and population to assess such, (1) type and duration of health and point, (2) special target population such children, pregnant women, (3) ecological effects. Comparative risk assessment is important to help to prioritize the solution of problem by distinguishing actual risk from potential exposure, and can help the regions to allocate the limited resources efficiently. The scale and cost of some risk has been conducted to demonstrate that the practical application can enhance the project design without being overly resource-intensive.

According to Walewski and Gibson [6], risk is often referred to as presence of potential treats and opportunities that influence the objective of project during construction, commissioning, and use of time and it also become an exposures to the change of occurrences that affecting to the project objective. Traditional risk assessment has been related with the probabilistic analysis that requires events to be mutually, exclusive, exhaustive, and conditionally independent. Determinations of risk are difficult to determine. There are 4 mitigation strategy that will help to decrease the risk, such : (1) avoidance, when the risk is not accepted from several alternatives, (2) retention, when the decision made to accept the consequences, (3) control when the process continually monitor, and (4) transfer, when the risk is shared with others.

Manuscript received 1 March 2011; accepted 15 April 2011; published 1 May 2011.

B. Gunawan and Merry are alumnis from the Department of Computerized Accounting, Binus University, Jln. K.H Syahdan No 9, Kemanggisan, Palmerah, Jakarta Barat. E-mail:
Nelly is a faculty member of the Department of Computerized Accounting, Binus University, Jln. K.H Syahdan No 9, Kemanggisan, Palmerah, Jakarta Barat. E-mail:

According to Fletcher [2], Risk assessment to help the management to make a decision that necessary in the formal decision making and has significantly increased the number of issues relevant to covers the impact of target species. Quantitative risk assessment allowed the advisory to link their recommended action to the probability and it can be highly robust, but they require a significant level of information that in the small situation. The key element of any valid risk analysis is having the procedure to determine the appropriate consequences and likelihood levels.

For this risk assessment will use the Octave-S approach as a method. According to Alberts et al.l [1], the preparation of Octave-S are important to successful the evaluation, and before that, there are some key success factor : (1) getting senior management sponsorship for the evaluation (2) selecting the analysis team to lead the evaluation (3) setting the scope of evaluation. Setting the Octave-S approach requires developing of shared understanding of the goal's evaluation; this goal might be reduce the risk of major incident in the future and help to set the expectations and provides valuable information when the analysis team subsequently sets the scope of evaluation. Octave-S is not a typical vulnerability evaluation that focus solely on technological issues, but it was an operational risk evaluation that similar to the typical business process or management evaluation.

According to Panda [3], Octave-S is one such framework that enables the organization to understand, assest and it is not a product but a process to identify the information of security risk, and help the organization to develop the qualitative risk and identify the assets that are critical to the mission of organization. To manage risks, the Octave-S needs a comprising principles, attributes, and outputs. Attributes are derived from principles and tangible element, then output is a result to be achieved.Octave – S designed for the large organization and it optimize the process of assessing information security risk so the organization can obtain sufficient results with a small investment in time, people and other sources.

4. Analysis Result from the IT risk

For the Octave-S approach, it will be divided in 3 phases, they are:

- Build asset- based threat profiles, will divide in two process such as identify organizational information –S1 and create threat profile –S2
- Identify infrastructure vulnerabilities, which there is one process: examine computing infrastructure in relation to critical assets – S3
- Develop security strategy and plans, which divided into two process : identify and analyze risk –S4, and develop strategy and mitigation plans –S5

In phase S1, we will identify the information from the company, the analyze from the company result, it will divide in 4 main steps, first analyze the qualitative evaluation on risk impact, which the company rarely find any complain from the client and business partner because the company have a high commitment to give the best service through the client. In the financial operation, company gain the spending 5-10% for every years because the increasing of material and will be impact to the receivable of the company. For the working hours, it increase in 30% if the company get any big project. The threat possibility of the employees in the company stay in the medium type because the job in the company will divide into two types, a field job and office job, which the field job is more risky. Last, the company have to pay the penalty if they late from the project due, but the penalty will be less than 100 millions. Second, company will identify the organizational asset, to support the company activities, company use Smartsys as a main system which this system will process the information about customer, vendor, sales, purchases, and another valid information. Third, practical evaluation security in company, it divided into 15th types evaluation result such: the security and training awareness of the employees, security strategies, security management, security roles, collaborative security management, possibility recovery plan from the disaster, physic access control, controlling and physically security auditing, System and networking management, Controling in IT security auditing, Approval and authorized, risky management, encryption, architecture and security design, and incident management.

Still in the first phase, for the S2 we will create the threat profile, it will divide into three steps. First, choosing the critical assets which according to Octave-S approarch the analyze team have to pick up 5 main asset in the whole of company and company choose Smartysys, which this asset are the most critical that used in the company. Second, security needs in critical assets, which it means the security of information, data integrity, and availibity of information. Third, threat identify of the critical assets, this step will divided into 4 steps:

- Access way, actor, motif, and threat's type. This step show the critical asset in the company by the network and physical. 2 actor will come from the internal and external company. There's also 2 motif which it happened with and without excuse.
- Defined of threat's actor, which in this company looking from Smartysys, e-mail, and design documentation. From physical access, the threat come from internal in modification and interruption, then from external come from disposal and interruption procedure
- Identified the potential threats. In Smartysys, the IT manager will maintain and update the server that threated by the virus, spyware and worm. In email, the IT manager will maintain the email server and user who's didn't log out the email. Last, for design documentation there's no threat come from network, but it come from internal and external company.

In the second phase, S3 will examine computing infrastructure in relation to critical assets, this process will have two main steps, they are:

- Checking the computer infrastructure. The nearest system to the critical asset in the company is Smartysys information system which is a system of interest. Smartysys divided into some component class, such servers, internal networks, and on-site workstations. This IS just using the Internal Network component to send the information and application to the peoples. All the person can access

the Smartysys in the On-site workstation class component. Storage device class component used to collect the information from Smartysys and backup it. No system and the other component who access the information or the application from Smartysys.

- Analyze the process related to the technology. The person who take a responsible to maintain and take care of the class component are IT manager and Smartysys outsource. LAN connection is the class component in the internal networks who has a related into Smartysys and email. Then, for On-site workstation class component, there's include a few items, such a PC accounting, PC Cost Control, PC designer, PC HRD, ad PC marketing. Which every item will connect to the email asset and smartysys, except the PC designer who not using the Smartysys but it connect to the design documentation. Every user in every item become the person who take a responsible in the item of class component with the support from the IT manager.

In third phase, for S4 process, it will identified and analyze the risk happened. This process have three main steps. First, evaluate the impact of threat. This step will serve the data about analyze team assessment from the impact will happened in every step and it will also look in a critical asset. For smartysys, a disposal from the sensitive data of Smartysys IS give the medium impact through the company reputation and low impact to the other criteria. This assessment available to access the network which physically, internal, and external with and without excuse. In email, the threat give the medium impact for the company's financial because the data sending by email was a sensitive data, if it get lost it will make the company loss. Then the medium impact also give into the disposal and interruption to the company productivity. Then for design documentation, there's no impact assessment in every threat type to the design documentation because all of this can be access by the network. Second, create the probability criteria evaluation, this step will make the analyze team to take the time of any threat happened which in a month for the highest period and one times in five years for the lowest. Third, evaluate the threat probability, in Smartysys the probability have a medium value from the internal which modification happened with and without excuse, and for the physic access have the medium value too which the external did without excuse through the threat interruption. In email, the threat come from internal with a medium probability and high probability for the threat come from external. Then for design documentation, threat in the low possibility from the internal and medium possibility from the external.

Still in third phase for the S5 process, it will develop strategy and mitigation plans, and it will take some steps:

First, the protection strategy have to be identified. This step describe how long the protection strategy in the company and every security practice have a stoplight status red which are: security practice no.4 about the roles of security and rights, security practice no.5 about collaborative security management, security practice no.11 about authorized and authenticity, and security practice no.12 about susceptibility management.

Second, selecting the mitigation approach. According to the risk profile in the questioner, spotlight took a place in the security practice. This area in the red zone because company hasn't had a security role and haven't ensure that improvement of security IS. And, Third, to develop the protection strategies for every practice in the red zone. There are five main practices, security practice no.4 about security and roles, security practice no.5 about collaborative security management, security practice no.11 about authenticity and authorization, security practice no.12 about susceptibility management, and security practice no.15 about incident management.

5. Conclusion

According to the research about risk assessment using Octave-S we can take some conclusion:

1. The identification of the critical assets in the company are : Smartysys IS which are a System of Interest, E-mail as a communication facility based on web include a necessary information of the company, and design documentation include to the intellectual product and that is an asset such a document
2. The result of questioner in the company show that the company have any weakness in five from fifteen security practices that mention in the Octave-S method such as ; security and roles, collaborative security management, authorized and authenticity, susceptibility management, and incident management.
3. Critical asset of company in the every susceptibility in the risk of threat :
   - Smartysys IS include network access have the biggest risk in the ongoing process include maintenance system, aspect of security information hasn't being maintance
   - Another critical assets, email based on internet and have an enough risk. This asset can be secure if there's any procedure and awareness of information security in the company
   - By documented the document based on IT, risk of losing and data thief can be reduced. Company can take a physical security to save the design documentation

References

[1] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "OCTAVE-S Implementation Guide, Version 1.0", Volume 2: Preparation Guidance, CMU/SEI-2003-HB-003, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA., Jan. 2005, from: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA453302

[2] W. J. Fletcher, "The application of qualitative risk assessment methodology to prioritize issues for fisheries management," *ICES J. of Marine Sci.*, vol. 62, pp. 1576-1587, Jul. 2005, from http://www.fisheries-esd.com/a/pdf/ICESv62p1576-587-%20ERA%20Article.pdf.

[3] P. Panda, "The OCTAVE® Approach to Information Security Risk Assessment," *ISACA Journal*, vol. 4, pp 37-41, Aug. 2009, from http://www.isaca.org/Journal/Past-Issues/2009/Volume-4/Pages/The-OCTAVE-Approach-to-Information-Security-Risk-Assessment1.aspx.

[4] A. Labriola, "Blasting Risk Assessment for Gunns Limited Proposed Pulp Mill Development Site, Tasmania," Orica Quarry & Construction Services, Revision 5, March 2005, from: http://www.gunnspulpmill.com.au/iis/V15/V15_A49.pdf.

[5] J. Moteff, "Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences," CRS Report for Congress Order Code RL32561, Sep. 2, 2004, from: http://www.fas.org/sgp/crs/RL32561.pdf.

[6] J. Walewski and G. E. Gibson, Jr., "International Project Risk Assessment: Methods, Procedures, and Critical Factors," The University of Texas at Austin, Austin, TX, Center Construction Industry Studies Report No. 31, Sep. 2003, from http://www.ce.utexas.edu/org/ccis/a_ccis_report_31.pdf.

[7] "Comparative Risk Assessment," in *Pollution Prevention and Abatement Handbook*, World Bank Group, Apr. 30, 1999, pp. 45–53, from: http://go.worldbank.org/E6G093QFZ1.