Critical Thinking in Various Risk Assessment Issues to Benefit Malaysian Small and Medium Sized Enterprises (SMEs)

Ryan Yang GUO[a], Su Yan LEE[b]

[a]Faculty of Computing and Information Technology
INTI University College, 71800 Nilai, Negeri Sembilan
Tel : 06-7982000, Fax : 03-7997636
E-mail : ryan_guo@intimal.edu.my

[b]Web and Media Design
UCSI University, 56000 Kuala Lumpur
Tel : 03-91018880, Fax : 03-91023605
E-mail : sylee@ucsi.edu.my

ABSTRACT

Information is the priceless assets in all size of businesses. This is widely accepted nowadays. In order to protect information away from the threats, it has becomes a very challenging job with the needs of comprehensive resources, it can be extremely difficult for Small and Medium Sized Enterprises (SMEs), not only because of they have lack of resources, they may have no ideas about the prioritized tasks. Risk Assessment however is the best way to make SMEs to have a clearer vision on where are they standing and how far they need to go. In this paper, we present some of our findings from a printed survey to illustrate the problems in the current practice on information security within Malaysian SMEs. Some questions in this survey are focused on identifying the problems on risk assessment faced by the Malaysian SMEs. In addition, we discuss the some advices in assisting SMEs to carry out risk assessment in a more effective and efficiency way.

Keywords

Example:
Information Security Management, Risk Assessment

1.0 INTRODUCTION

Abraham Lincoln had a very famous quotation: “if we could first know where we are and whither we are tending, we could better judge what to do and how to do it.” (Einhorn, 1992). In hundred years ago, his advice was not focused on information security management, however, after some continuous research carried out in the area of current practices on information security management among Malaysian Small Medium Sized Enterprises (SMEs) we have found Abraham’s idea goes along with information security management life cycle, where the first job is to identify the businesses’ existing security status. With the knowledge of this, we can only have better ideas to scratch a plan about how to meet security goals. In order to protect company’s assets, the most important task is to clearly understand what are the valuable assets need to be protected. Followed by identify the potential violation of security, known as threats and it is not necessary for the violation to actually occur to be a threat (Bishop, 2003). In this case, risk assessment comes in and plays a very critical role to determine whether the mentioned assets need to be protected, and in what kind of level should it be protected.

In ISO/IEC 17799, it defines risk as “Business risk is the threat that an event or action, which can adversely affect an organisation’s ability to successfully, achieve its business objectives and execute its strategies.” (ISO, 2000)

2.0 FINDINGS

A survey, which contains ten multiple choice questions was distributed in early 2008 and the main objectives includes: the understanding about risk assessment among the selected Malaysian SMEs; the current practice of risk assessment and how risk assessment stands in the map of information security management and the outcomes. With the effort to ensure the quality of research, the research strategy focuses on those SMEs with basic knowledge about information security management and/or risk assessment. For this reason, all the selected SMEs are doing E-Commerce or data exchanging to other businesses’ partners as part of their main business action. There are 65 companies contribute to this survey and submitted the valid feedback in mid-August 2008. All the participating companies are partners of Grand Dynamic Resource Sdn. Bhd. and they are tightly involved in E-commerce in their business. The survey covered fields of risk assessment, risk management, security education and training, incident management and so on. In this paper we will only discuss the findings relevant to this paper, the rest findings may be published in another paper.

In Figure 1, there are only 4 SMEs out of 65 SMEs clearly answers they have not done risk assessment in there company. Fortunately, 51 companies, which are 79% of our interviewers practiced "Risk Assessment" in there companies.

This result shows that at least for the local companies, who is dealing with E-Commerce/M-Commerce or data interchange are concern on carries out certain tasks or practices in information security management. The positive response to this question add in the urge to look into type of risk assessment in the participated SMEs.

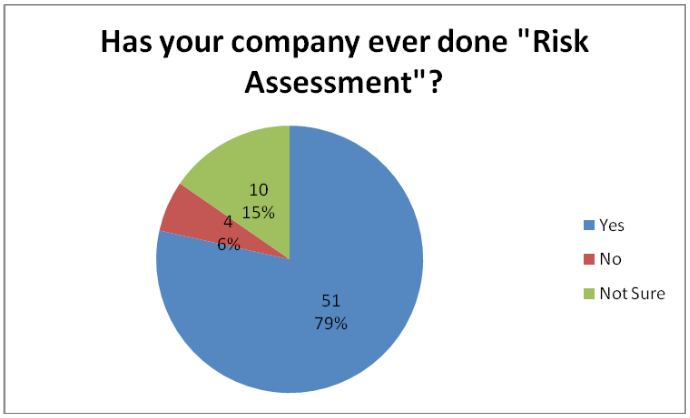

Figure 1: Survey Question 1 – Has your company ever done "Risk Assessment"?

Unfortunately, it shown on Figure 2, among the total of 51 SMEs, there are 40 SMEs, which are 78% claim that their company has just done once Risk Assessment by someone. Only 7 companies gave the clear answer that they are repeating Risk Assessment periodically, this finding shows that most of SMEs may think Risk Assessment is a one time job and they do not realized that risks can be changed when the business environment evolved through time, for example, a new added technology may affects the company's security strategy and the analysis of risk assessment may have some kinds of differences.

Another important finding from this research is about how does the SMEs carry out Risk Assessment, are SMEs able to carry out Risk Assessment by themselves or they need a help from this technical partner or the information management team is organised by both parties? In Figure 3, it clearly shows that out of 47 SMEs, which have done at least once Risk Assessment within the company, there are 44 feedbacks indicate this job is fully or partially conducted by the third party which indicate 93.6% of outsource reference.

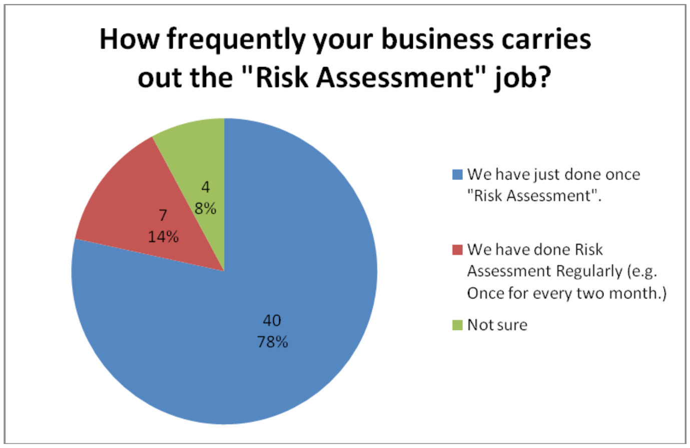

Figure 2: Survey Question 2 - How frequently you business carries out the "Risk Assessment" job?

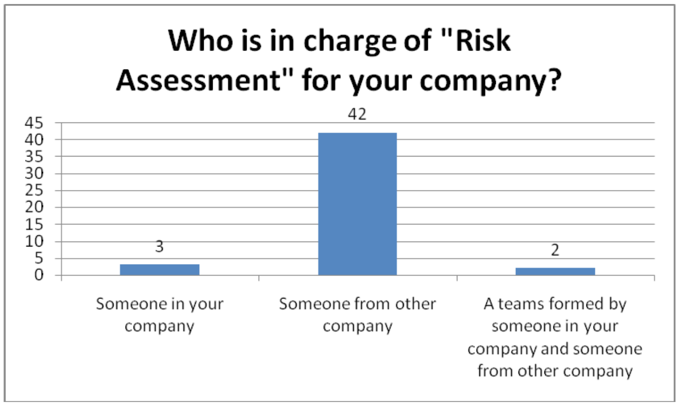

Figure 3: Survey Question 5 – Who is in charge of "Risk Assessment" for your company?

From the findings shown above we found that among the SMEs which done Risk Assessment is often lack of knowledge in the whole information security management life cycle (ISO, 2005). This may due to various reasons, includes some of common misunderstandings such as, Risk Assessment is a process which only need to be done once; Risk Assessment tools/software are extremely costly; Risk Assessment can be only taken by some security experts with ten and more years relevant experiences, and many more.

3.0 RECOMMENDATION ON RISK ASSESSMENT FOR MALAYSIAN SMEs

There are many different methodologies may helps in Risk Assessment such as NIST SP 800-30/NIST SP800-66, Facilitated Risk Analysis Process (FRAP), OCTAVE, CRAMM and Spanning Tree Analysis (Harris, 2008). However, none of these strategies will fully fits into Malaysian

SMEs risk assessment context whereby the resources may be lack in compare to those available for SMEs in US and EU. A simplified guideline is seems more practical and this shall helps to change their mindset on Risk Assessment. Continuous and regular Risk Assessment will be more effective to find out the real security risks. In addition, for most of cases, SMEs can actually take the risk assessment by using their own resources. Security experts have the required technical knowledge in information security but may not have sufficient knowledge about how the business runs, in other words, they do not know much about SMEs' culture, politics and policies. There are few Risk Assessment tools or framework which is free and some are web based tools, they may not even need to be installed.

3.1 Risk Assessment is a "Continuous" Task

Security risks may change with time, for example, if a company's network engineers switch of the wireless router, there should no risk of potential attacks from other mobile devices since they can only connect to company's network by using wired connection. However, assumption can be made, if a staff bring in his own wireless router and connect to his PC, the risks are changed.

This example just proves Risk Assessment can not be treated as a single step of process. The more Risk Assessment tasks take in the company, we should have more useful information in our hands and this can be very critical first hand references when the company wants to design, amend, or upgrade their information security plans or policies.

Controversially, some SMEs claim that they have done Risk Assessment regularly, once every two months, however, they always receive the same result and top management may consider these repeating works are wasting their time and resources. In our research, we carried are on site observation and interview within the companies. Too regular assessments may result in the useless result, namely because the date and time of assessment have been made known to the company's employees. Employees will be very alerted in this short period, for example they shuts off chatting software, peer-to-peer downloading software, and so on. When the SMEs take our recommendation and takes "irregular" Risk Assessment, the feedback returned from them are all positive.

3.2 Irregular Risk Assessment

In order to reflect the current situation, there is a need of strategy. Regular risk assessment, as we mentioned above, to carry out risk assessment on the fixed day such as the first day of each month will always lead a inaccurate output in most of cases, especially if the end users know this task is going to be carried out in a particular day. The process of identifying the user's behavior is difficult as each user behaves differently in search of software's loopholes.

Irregular risk assessment means to process a risk assessment on a scheduled but not by a fixed date and/or a fixed time. It can be randomly chosen to any day and the assessment can be carried out in the morning or afternoon. The key is never to let the end user know someone is going to do Risk Assessment.

3.3 Should Risk Assessment be an "In Source" Process or an "Out Source" Process

From the survey and onsite interview, we found the majority of Malaysian SMEs are either never done Risk Assessment or have done it by paid services from third parties. To answer the question why most of Malaysian SMEs consider out source the information security management is because it is not an easy job, the company do not wish to employ a full-time security expert, most of employers or IT managers do not realize information security management is a ongoing development, their common sense is security related software must be very costly, and so on.

To set a well-designed security plan needs a strategy and requires wide covered knowledge and experiences so the initiating tasks can be out source to a security company. However, it is very uncommon for a third party to monitor the daily security for a SME. Furthermore, every company is best to know itself. This is extremely important since security concerns must become a part of companies' culture. Hence, the only barrier left is whether are there any cost-effective softwares can be used to help SMEs for their Risk Assessment.

3.4 Tools for Risk Assessment

The process of risk assessment is generally divided into two main steps. Firstly it should be focused on a higher level then followed by a more specified level to test more detailed security risks (ISO, 2000). However, to carry out the higher level of risk assessment requires knowledge on both information security management concepts and practical experiences. Nevertheless, the high level of Risk Assessment needs not to be repeated as frequent as the lower level Risk Assessment. Through our interview to the selected Malaysian SMEs we have found there are quite numbers of SMEs have the ability to practice low level Risk Assessment by themselves. The tools we suggest here are more toward on helping in lower level Risk Assessment.

Automated Security Self-Evolution Tools (ASSETs) is one free and web-based application developed by researchers from University of Georgia, USA and it fully complies with NIST 800-26 Security Self Assessment Guide for Information Technology Systems (Gatewood, 2007 and NIST, 2001).

In addition, there are always alternative solution which is cheaper but effective. For example, there are various free security tools can be used to analysis specified security risk, such as network penetration test could possibly disclose a potential harmful network vulnerabilities, web scanner tools can perform comprehensive test on Web servers; sectools.org provides hundreds of powerful tools and covered almost all security aspects (Insecure, 2009).

3.5 Be a Part of International/Local Security Research

SMEs are always saying they have faced constraints on lack of expertise. One of a cost-effective way to overcome this problem is to get themselves involved in academic and/or government research. Malaysian Super Corridor (MSC) and Multimedia Development Corporation (MDeC) provides seminars such as 2008 Capability Development Programme (CDP) to promote and share information on how a company can comply with international standard which include ISO 27001 (MSC, 2009). Another example is Malaysian Institute of Microelectronic System (MIMOS) and Malaysian Communications and Multimedia Commission (MCMC), which are also independent parties sharing their recent information/cyber security related research with local SMEs (MIMOS, 2009 and MCMC, 2009).

Some international and/or domestic organization like Cybersecurity.my carries some information security relevant research. They welcome any local SMEs to be participant themselves as part of their research (Cybersecurity, 2009). In addition, they are often to share their recent findings and research papers online, so that SMEs could possibly learn from other companies' experiences.

Researchers in local academic institution like those who are doing PhD or other types of research are very keen to study and to have an onsite analysis in many different aspects on Information Security Management for SMEs. They are looking for some company to have a long-term relationship in order to achieve their research goals.

4.0 CONCLUSION

In this paper, we discuss about a few of our recent findings which expose the problems about the current practice of Risk Assessment among Malaysian SMEs. Moreover, the discussed suggestions in this paper could possibly help local SMEs to open up their company on more available options to conduct risk assessment.

This is a continuous research and authors are closely linked with some MSC status companies. The research is still carrying on and the full findings in the mentioned survey will be published in another paper.

REFERENCES

Beachboard, J., Cole, A., Mellor, M. Hernanez, S. and Aytes, K. (2008), *Improving Information Security Risk Analysis Practices for Small- and Medium- Sized Enterprises: A Research Agenda*, The Journal of Issues in Information Science and Information Technology, vol. 5, 99-101.

Bishop, M. (2003). *Computer Security Art and Science*, Boston, Pearson Education.

Cybersecurity, (2009), *Cybersecurity Publication*, Retrieved January 10, 2009 from http://www.cybersecurity.my/en/knowledge_bank/papers/papers/main/detail/183/index.html

Einhorn, L. J. (1992), *Abraham Lincoln, the Orator: Penetrating the Lincoln Legend*, Greenwood Press, London.

Elizabeth, C. and Overill, R. (2007), *The Design of Information Management Systems for Small-to-Medium Size Enterprises*, 6th European Conference on Information Warfare and Security (ECIW 2007). Shrivenham, UK.

Gatewood, S. (2007), *Automated Security Self-Evaluation Tools (ASSETs)*, Retrieved December 27, 2008 from

http://www.sacubo.org/sacubo_resources/best_practices_files/2007_files

Harris, S. (2008). *CISSP All-in-One Guide,* 4th ed. New York: McGraw-Hill.

ISO, (2000), *Information Technology – Code of Practice for Information Security Management*, ISO/IEC 17799, International Standard Organisation, Geneva.

ISO, (2005), *Information Technology – Code of Practice for Information Security Management*, ISO/IEC 27001, International Standard Organisation, Geneva.

Insecure, (2009), *Top 100 Security Tools List Released*, Retrieved January 20, 2009 from http://insecure.org

MCMC, (2009), *MCMC Published papers*, Retrieved January 20, 2009 from http://www.skmm.gov.my/facts_figures/papers/index.asp

MIMOS, (2009), *MIMOS Press Release*, Retrieved January 20, 2009 from http://mimos.my/index.php?sub=3&ma=14

MSC, (2009), *MSC Malaysia Status Companies Honoured*, Retrieved January 23, 2009 from http://cdp.msc.com.my/news_archive_detail.php?mainID=005&subID=00022&id=406

NIST, (2001), *Security Self-Assessment Guide for Information Technology Systems*, NIST 800-26, National Institute of Standards and Technology, U.S.

Shah, J. (2006). *Information System Risk Assessment Methods*, Southwest Decision Sciences Institute Thirty-Seventh Annual Conference.