DYNAMIC MODEL FOR RISK ANALYSIS OF PICTURE ARCHIVING COMMUNICATION SYSTEM (PACS) AT HOSPITAL SELAYANG

NAZROOL BIN OMAR

UNIVERSITI TEKNOLOGI MALAYSIA

DYNAMIC MODEL FOR RISK ANALYSIS OF PICTURE ARCHIVING COMMUNICATION SYSTEM (PACS) AT HOSPITAL SELAYANG

NAZROOL BIN OMAR

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Centre for Advanced Software Engineering
University Technology Malaysia

NOVEMBER 2008

ABSTRACT

Risk analysis is the best method for every organization to secure their business environment from any undesired hazardous events such as malicious code attack or natural disaster that could cause a lot of loses and impairs business operation. Risk analysis is very important and necessary because the probability of a disaster occurring in an organization is highly uncertain. Hence, the prediction through analysis process is mandatory. Selecting methodology for information security risk analysis is crucial. This project analysis will follow ISO/IEC 27005 Information Security Risk Management Standard. This standard has been widely used as baseline or references by many commercial risk analysis tool developers. The risk analysis is carried out on Pictures Archiving and Communication System (PACS) of Hospital Selayang. The analysis attempts to identify and list the risks that might shut down the system operation and subsequently presented in Dynamic Fault Tree (DFT) as a dynamic model. Dynamic Fault Tree is a method that extends standard fault trees by allowing the modeling of system risks behaviors and interactions with each other over a period of time. At the end of the project risks register will be produced in the form of report. The risk report will benefit Hospital Selayang during overall risk assessment of the Pictures Archiving and Communication System (PACS).

ABSTRAK

Penganalisaan risiko merupakan satu kaedah terbaik bagi sesebuah organisasi untuk memastikan persekitaran perniagaan selamat daripada ancaman merbahaya seperti serangan pengodam atau bencana alam yang boleh menyebabkan perniagaan tergendala sekaligus menyebabkan kerugian yang besar. Penganalisaan risiko sangat penting dan perlu disebabkan oleh kebarangkalian untuk sesuatu bencana itu berlaku dalam organisasi adalah sangat tidak menentu. Justeru satu kaedah ramalan melalui proses analysis perlu dilakukan. Pemilihan kaedah untuk proses analisa risiko perlu dibuat dengan berhati-hati. Analisis dalam projek ini *adalah ISO/IEC 27005 Information Security Risk Management Standard.* Standard ini telah digunakan secara meluas sebagai penunjuk aras dan rujukan oleh ramai pembangun alatan analisa risiko komersial. Penganalisaan risiko dijalankan kepada *Pictures Archiving and Communication System (PACS)* di Hospital Selayang. Analisa cuba untuk mengenalpasti dan menyenaraikan risiko-risiko yang boleh menyebabkan sistem tergendala dan kemudian dimodelkan dalam *Dynamic Fault Tree (DFT)* model. *Dynamic Fault Tree* merupakan satu kaedah yang memperbaharui standard Fault Tree dengan menunjukkan perhubungan antara satu risiko dengan risiko yang lain dalam satu tempoh masa yang tertentu. Di akhir projek ini nanti, satu daftar risiko akan dihasilkan dalam bentuk laporan. Laporan ini akan memberi manfaat kepada Hospital Selayang semasa penilaian risiko yang menyeluruh dibuat pada *Pictures Archiving and Communication System (PACS)*.

TABLE OF CONTENTS

CHAPTER 1

PROJECT OVERVIEW

1.1 Introduction

The growth of e-health services such as online medical advice, online pharmacies, and online patient record; both in public and private medical sector are inevitable. The proliferation and dependency of medical online system in healthcare sector in Malaysia has fueled up the need to protect the systems from any kind of threat to ensure the continuity of the healthcare services. It is acknowledged how important for a business to implement information security management in securing their ICT assets in order to staying in business, no matter in what circumstances befall. The primary process in information security management is risk analysis; a process to identify threats and vulnerabilities, analyze them to ascertain the exposures, and highlight how the impact can be eliminated or reduced. Risk analysis will provide a basis for risk evaluation, risk treatment and risk acceptance.

This project focuses on analyzing the risk faced by ICT based health institution that runs several ICT systems to support their daily operation. Hospital Selayang is chosen as the subject because it is the first public hospital in Malaysia that fully implemented with Total Hospital Information System (THIS). Pictures Archiving and Communication System (PACS) is one of the system that runs under THIS.

This project is outlined in six chapters. The first chapter is for project overview. Chapter 2 transcribes literature review and chapter 3 provides research methodology which consists of project development method and technique. Chapter 4 describes flow of risk analysis design. Chapter 5 presents implementation and result of this project. Chapter 6 provides conclusion of this report which covers summary of research finding and contribution of this research.

In this chapter, the report is organized into seven topics. It is started by introduction of this project paper and followed by background of problem, problem statement, project aim, project objectives, and project scope. This chapter is ended by chapter summary.

1.2 Background of problem

Hospital Selayang (SH) is an ICT-based hospital. It is located in Selayang, Selangor and equipped with 960 inpatient beds and 20 clinical disciplines. It has been designed and constructed for a Total Hospital Information System (THIS) environment. It is the first hospital in Malaysia and the world to operate with THIS which covers all aspects of hospital operation. The ultimate aim of this hospital is to be paperless and filmless hospital. It is critical to ensure THIS always in continuous operation. Therefore, security is very important and plays a vital role in protecting THIS asset and information. It was obvious that risk analysis is a method in determining which countermeasures need to be implemented in fighting against wide range of potential threats.

1.3 Problem Statement

There are many questions regarding the risk analysis outcomes but for this project, it will address and answer some problems that as stated as follows:

a. Examine what are potential threats for Pictures Archiving and Communication System (PACS) that needs to be comprehensively identified and analyzed.

b. To identify critical asset that potentially exposure to loss as well incident that likely to happen if the asset is compromised by the threat.

c. Proper vulnerability investigation must be conducted to search and determine for flaws and weakness exist in Pictures Archiving and Communication System (PACS) environment.

d. To study and determine Dynamic Fault Tree (DFT) model can be used to model the information security risk in dynamic model.

1.4 Project Aim

The aim of this project is to perform risk analysis on the Pictures Archiving and Communication System (PACS) and to model the identified risks using dynamic model method called Dynamic Fault Tree (DFT) modeling technique. The analysis will be based on ISO/IEC 27005 Information Security Risk Management Standard. The analysis shall benefit Hospital Selayang in overall risk management process especially in determining what controls are needed to reduce the risks to an acceptable level.

1.5 Project Objectives

The objectives that will be specified below explain what kind of knowledge the study is expected to obtain. It also should give a clear notion of what is to be described, determined, identified and analyzed.

a. To study existing and potential threats in Pictures Archiving and Communication System (PACS).

b. To carry out risk analysis to Pictures Archiving and Communication System (PACS) and asset related to it based on suitable technique.

c. To determine whether dynamic system modeling can be used in information security risks.

d. To produce risk analysis report which consists of risk identification and risk estimation details as an input for Hospital Selayang to be used in their overall risk management process.

1.6 Project Scope

Project scope will indicate the limitation of this project in terms of its process, coverage, collaborators, participants and potential products.

a. The unit of analysis is Hospital Selayang which is located in Gombak, Selangor, a health institution.

b. The risk analysis is conducted on Pictures Archiving and Communication System (PACS).

1.7 Summary

This chapter has described introduction of this project report, background of problem, problem statement, project aim, project objectives and project scope. These topics have clearly stated and justify why this project is worth developed and implemented. Next chapter will discuss literature review.

REFERENCES

International Organization for Standardization, 2008. “ISO/IEC 27005 Information Security Risk Management Standard”. ISO Publication.

Council of Standards Australia, 1999. “*AS/NZS 4360:1999 Australian Standard Risk Management*”. Standards Association of Australia.

Gary Stoneburner, Alice Goguen, and Alexis Feringa, 2002. “*NIST - Risk Management Guide for Information Technology Systems*”. NIST Special Publication 800-30.

Joanne Bechta Dugaan, Tariq Said Assaf, 2003. “*Dynamic Fault Tree Analysis of a Reconfigurable Software System*”. University of Virginia.

Hong Xu, 2004. ”*Combining Dynamic Fault Trees and Event Trees for Probabilistic Risk Assessment*”. University of Virginia, Charlottesville.

Hichem Boudali, Pepijn Crouzen, and Mariëlle Stoelinga, 2007. “*Dynamic Fault Tree Analysis using Input/Output Interactive Markov Chains*”. University of Twente.

Geoffrey H. Wold and Robert F. Shriver, 1997. “*Risk Analysis Techniques”*. Disaster Recovery Journal.

Ian P. Leistikow, Geert H. Blijham, 2005. “*System-based risk analysis in healthcare*”. University Medical Center Utrecht.

Major Marc A. Lee, 2007. "*A Dynamic Systems Simulation Approach to Risk Mitigation for Critical Infrastructure*". United States Military Academy.

James W. Meritt, 2005. "*A Method for Quantitative Risk Analysis*". CISSP.

Jim Wang, 2003. "*Modeling Techniques for a Risk Analysis Methodology for Software Systems*". Carnegie Mellon University.

Gary Leonard Cave, 2002. "*Qualitative Analysis, Methodologies in the USA*". Entomologist, USDA-APHIS.

Dr. Doreen Watler, 2002. "*Qualitative Risk Analysis: Methodologies And Applications In Canada*". Canadian Food Inspection Agency.

L. Baliwangi, H. Arima, K. B. Artana, K. Ishida, 2007. "*Risk Modification Through System Dynamics Simulation*". Kobe University Japan, Kampus ITS Keputih Surabaya.

Alfredo Moscardini, Mohamed Loutfi and Raed Al-Qirem, 2007. "*The Use of System Dynamics Models to evaluate the Credit Worthiness of firms*". University of Sunderland.

Jean-Peter Ylén, 2007. "*System Dynamic Model For E-Commerce Customer Retention Strategy*". Technical Research Centre of Finland VTT.