DYNAMIC RISK MANAGEMENT APPROACH USING IMMUNE SYSTEM

AZADEH SARKHEYLI

UNIVERSITI TEKNOLOGI MALAYSIA

DYNAMIC RISK MANAGEMENT APPROACH USING IMMUNE SYSTEM

AZADEH SARKHEYLI

**A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Science (Information Technology - Management)**

**Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia**

JUNE 2011

To my dearly loved family and friends
To my respected supervisor

Thank you for all the sacrifices.

ACKNOWLEDMENT

Dr.Norafida Binti Ithnin, shows the way, gives my patience and the will to supervisor for this dissertation. I would like to express my greatest gratitude to my supervisor for her great support and guidance in helping me to complete the thesis. I also would like to give my appreciation to my sisters, for collaborating me to do this thesis and my parents, over the years they have continued to support and motivate me in my studies. Not to forget, my friends who helped me directly or indirectly.

ABSTRACT

Risks include the factors that might adversely affect on project outcomes. Risk analysis includes the processes concerned with identifying, analyzing and developing security strategy and plans for the factors. Although currently there are methodologies known such as *(CCTA Risk Analysis and Management Method (CRAMM)* or *Consultative, Objective and Bi-functional Risk Analysis (COBRA)* etc. for Risk Management, they have common failure for instance no specific function which recover/avoid risks/attacks toward IS/IT component and poor executive support, high cost of implementation, untimely response, insufficient accountability, inability to qualitatively measure control environment, infrequent in assessment, inaccurate data. Hence, these problems and the importance of IS/IT Risk Management cause the research to organize a dynamic risk management approach by making them intelligent as like as the immune system which is a complete system and could be the best model for simulating Risk Management in the organizations. However, the results of this study could help organizations toward improving IS/IT Risk Analysis process which are designed and proposed by investigation about their current procedure and problems of Risk Management.

ABSTRAK

Risiko termasuk faktor-faktor yang mungkin memberikan kesan berlawanan terhadap hasil projek. Analisis risiko mengambil kira proses mengenal pasti, menganalisis dan membina strategi dan pelan keselamatan untuk faktor-faktor tersebut. Walaupun di masa kini terdapat kaedah-kaedah seperti *(CCTA Risk Analysis and Management Method (CRAMM)* atau *Consultative, Objective dan Bi-functional Risk Analysis (COBRA)* dan sebagainya untuk Pengendalian Risiko, namun kaedah-kaedah ini mempunyai kelemahan seperti ketiadaan fungsi yang spesifik yang boleh mengelak risiko atau serangan terhadap komponen IS/IT serta fungsi sokongan eksekutif yang lemah selain kos perlaksanaan yang tinggi, respon yang tidak dapat diramal, kelemahan dalam kebergantungan, ketidakbolehan mengukur persekitaran kawalan secara kualitatif, penilaian yang jarang dibuat serta data yang tidak tepat. Maka, masalah-masalah yang ada serta kepentingan Pengendalian Risiko IS/IT telah menjadi pemangkin kajian ini untuk mengendali satu pengendalian risiko yang dinamik dengan menjadikan ia sebaik system ketahanan yang merupakan system yang lengkap. Sistem ini boelh dijadikan model untuk simulasi Pengendalian Risiko dalam sesebuah organisasi. Justeru, hasil kajian ini mampu membantu organisasi-organisasi meningkatkan proses Analisa Risiko IS/IT yang direka dan dicadangkan melalui penyiasatan mengenai prosedur dan permasalahan Pengendalian Risiko yang terkini.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

RM	Risk Management
IT	Information Technology
IS	Information System
CRAMM	CCTA Risk Analysis and Management Method
COBRA	Consultative, Objective and Bi-functional Risk Analysis
BS	British Standards
ANFIS	Adaptive-Network-based Fuzzy Interface System
LVQ	Learning Vector Quantization
ANN	Artificial Neural Network

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

This study tries to do IT Risk Management using Immune System, because of this at first Immune system as the main system, which this research wants to investigate base of it, will be described. After that try to answer the main question, it means that why Immune system have chosen for this project. Another question is related to how this study can improve Risk Management process for achieving better result. So, Risk Management process and how can give these process, will be defined as secondly in this section.

Immune system is a complex network of cells, tissues, and organs designed to defend the body against germs, viruses, and other form of body toxins. Immune system alerts body's defenses and calls to action the natural processes that keep the body safe and healthy [1].

Like nature, the body has the natural ability to protect and heal itself. This happens through the immune system. Research shows a healthy immune system helps prevent most common illnesses.

The secret to the success of immune system is an elaborate and dynamic communications network. Millions and millions of cells, organized into sets and subsets, gather like clouds of bees swarming around a hive and pass information back and forth. Once immune cells receive the alarm, they undergo tactical changes and begin to produce powerful chemicals. These substances allow the cells to regulate their own growth and behaviour, enlist their fellows, and direct new recruits to trouble spots [2].

About Risk Management, it is clear that risks include any factors which might adversely affect project outcomes. Risk management includes the processes concerned with identifying, analyzing and responding to uncertainty to those factors that might adversely affect project outcomes [4]. An understanding of risk management is essential for any worker involved in a project, paid or unpaid, because each person is legally and ethically responsible for contributing to this process for being aware of, and minimizing the potential for risk in any given situation. The focus on risk management has emerged as a result of cases where there has been a failure to identify or respond to risk, resulting in accident, or other loss. Risk management has become a formalized approach which helps to ensure that workers and organizations are accountable for all activities and responses, thereby minimizing the consequences of adverse events. Risk management can also play a role in maximizing the results of positive events [6].

However, a Risk Process, or Risk Management Process, describes the steps that need to take to identify, monitor and control risk. Within the Risk Process, a risk is defined as any future event that may prevent to meet the team goals. A Risk

Process allows identifying each risk, quantifying the impact and taking action now to prevent it from occurring and reduce the impact should it eventuate.

Generally six steps proposed for Risk Management such as identify any hazards, identify the risks associated with those hazards, assess the risks, control the risks , document the process, Monitor and review the outcomes.

Although the process of Risk management which are exist in current organization used extremely for protection of their resources and productions, the importance of this subject and the common failure which are acquired in current methodologies cause the study focused to Risk Management using a complete system which tasks are similar and exist in nature, that is Immune System. So this research can simulate an organization with a human body. Consequently by investigation of the component of Immune Systems and study about their procedure and problems of Risk Management the study can design and propose tools for improving IT Risk Management.

1.2 Statement of Problem

Some problems are specified in current Risk Management methodologies that are used in organizations, they are common between them such as there is no specific function which recover/avoid risks/attacks toward IS/IT component, poor executive support, high cost of implementation, untimely response, insufficient accountability, inability to qualitatively measure control environment, infrequent in assessment, inaccurate data.

1.3 Objectives of the Study

1. To study the existing method of Risk Management
2. To investigate the concept of Immune System
3. To design and propose a Risk Management process to embedding the concept of immune system
4. To develop the proposed Risk Management process

1.4 Research Questions

Main research question:

How to improve Risk Management process using Immune System approach?

Sub research questions:

1. What are the components inside the Immune System?
2. How to map Risk Management process by Immune System component?
3. What is the impact of the Risk Management process on attacks?

1.5 Scope

Selected Risk Management methodologies are CRAMM, RUSECURE, OCTAVE, OCTAVE-S, BS. And selected symbol for simulation is Immune System. Another thing is development of the proposed risk management process which MATLAB software will be used.

1.6 Significance of the Study

Currently there are known methodologies (CCTA Risk Analysis and Management Method (CRAMM) or Consultative, Objective and Bi-functional Risk Analysis (COBRA) and so on) for Risk Analysis/Management, but they have common failure.

1. There is no specific function which recover/avoid risks/attacks toward IS/IT component
2. Poor executive support
3. High cost of implementation
4. Untimely response
5. Insufficient accountability
6. Inability to qualitatively measure control environment
7. Infrequent in assessment
8. Inaccurate data

These failure and importance of IS/IT Risk Management cause the research tries to simulate Immune System of human body with an organization because this system is complete and consider a lot of aspects of immunity. However the findings of this study are important to help organizations toward IS/IT Risk Management process which will be designed and proposed by using Immune System.

REFERENCES

1. Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont," An Artificial Immune System Architecture for Computer Security Applications" , IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION, VOL. 6, NO. 3, JUNE 2002.
2. P. D. Williams, "Warthog: Toward an artificial immune system for detecting 'low and slow' information system attacks," M.S. thesis, Air Force Instit. Technol., Wright-Patterson AFB, OH, Mar. 2001.
3. Richard A. Gonçalves, Carolina P. de Almeida, "A cultural immune system for economic load dispatch with non-smooth cost functions", Proceeding ICARIS'07 Proceedings of the 6th international conference on Artificial immune systems Springer-Verlag Berlin, Heidelberg 2007.
4. Boon Siong Neo, Kewong Sin Leong,"Managing Risks in Information Technology Projects" Journal of Information Technology Management, Volume V, Number3,1994
5. Golfried B.Williams_University of East London UK , "Online Business Security Systems" Springer Science+Business Media, LLC 2007.
6. Shon Harris, "CISSP All-in-One Exam Guide" Fourth Edition, by the McGraw-Hill Companies, 2008.
7. You Lu ; Xin Yang ; "Design risk management--the guarantee of product innovation", 9th International Conference of Computer-Aided Industrial Design and Conceptual Design,IEEE. CAID/CD 2008.
8. Boehm, B.W., 1991. Software Risk Management: Principles and Practices, IEEE Software, No. 1, pp. 32-41, IEEE CS Press.

9. Carol Woody_ Carnegie Mellon University, “Applying OCTAVE” is sponsored by the U.S. Department of Defense, May 2006.
10. Richard A.Caralli, James F.Stevens, William R.Wilson ”Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process”, Software Engineering Institute from Carnegie Mellon University, May 2007.
11. Gary Stoneburner, Alice Goguen, and Alexis Feringa,” Risk Management Guide for Information Technology Systems” NIST Special Publication 800-30, 2002.
12. Risk Management by ARMY, MARINE CORPS, NAVY, AIR FORCE, february 2001.
13. Risk Management Tools, by Michael A. Greenfield Deputy Associate Administrator Office of Safety and Mission AssuranceLangley Research Center May 2, 2000.
14. Risk Management Guide for Information Technology Systems, Recommendations of the National Institude of Standards and Technology, 2002.
15. Risk Management byJames W. Meritt.
16. Christopher Alberts, Audree Dorofee, Carol Woody_ Carnegie Mellon University,”Introduction to the OCTAVE Approach” is sponsored by the U.S. Department of Defense August 2003.
17. E. Henley, H. Kumamoto(1996). Probabilistic Risk Assessment 2nd edition, IEEE Press, New York.
18. Paulina, Januszkiewicz ; Marek, Pyka ;” Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology”, The Second International Conference on Availability, Reliability and Security IEEE. ARES 2007.
19. Maglogiannis, I.; Zafiropoulos, E.;” Modeling Risk in Distributed Healthcare Information Systems”, Engineering in Medicine and Biology Society. EMBS '06. 28th Annual International Conference of the IEEE, 2006.
20. J. O. Kephart, G. B. Sorkin, M. Swimmer, and S. R. White, “Blueprintfor a computer immune system,” in Proceedings of the Virus Bulletin International Conference. Abingdon, U.K.: Virus Bulletin Ltd., 1997.
21. Alwi, N.H.M.; Ip-Shing Fan; “Information security management in e-learning”, Internet Technology and Secured Transactions IEEE. ICITST 2009.
22. "CRAMM Management Guide" by Security Service on behalf of the UK Government.

23. http://www.compservis.lt/cramm/index.php?Lang=5&ItemId=34625Source: www.cramm.com.
24. Briand, L.C.; El Emam, K.; Bomarius, F.;” COBRA: a hybrid method for software cost estimation, benchmarking, and risk assessment ”, International Conference on Software Engineering, IEEE. Proceedings of the 1998.
25. http://rusecure.rutgers.edu/cybermonth.
26. http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030166440.
27. Handbook of Information Security Management, Domain3,"Risk management and Business Continuity Planning,"Micki Krause and Harold F.Tipton,editors(CRC Press LLC): www.cccure.org/Documents/HISM/223-228.html.
28. http://arm-group.net/RiskManagement/Default.aspx.
29. British Standard BS6079:1996"Guide to project management", British Standards Institute, ISBN 0-580-25594-8,1996.
30. http://www.electroresponse.com/1100/index.htm.
31. S. A. Hofmeyr and S. Forrest, “Immunity by design: An artificial immune system,” in Proceedings of the Genetic and Evolutionary Computation Conference. San Mateo, CA: Morgan Kaufmann, July 1999, pp.1289–1296.
32. D. Dasgupta, Ed., Artificial Immune Systems and Their Applications, Heidelberg, Germany: Springer-Verlag, 1999.
33. Guangfu Wei ; Xin Xhang ; Xinlan Zhang ; Zhifang Huang ;” Research on E-government Information Security Risk Assessment - Based on Fuzzy AHP and Artificial Neural Network Model” First International Conference on Networking and Distributed Computing (ICNDC) IEEE, 2010.
34. Fundamentals of Neural Networks, Architectures, Algorithms , and Applications, Laurene Fausett , Prentice-Hall, Inc. Upper Saddle River, USA, 1994, ISBN: 0-13-334186-0.
35. Artificial Neural Networks , Ajith Abraham, Oklahoma State University, USA, Handbook of Measuring System Design , 2005, John Wiley and Sons, ISBN: 0-470-02143-8.
36. ANFIS: Adaptive-Neural Network Based Fuzzy Interface System, Jyh-Shing Roger Jang, 1993, IEEE Transactions on systems, Vol 23, No 3.
37. A Statistical Approach to Neural Networks for Pattern Recognition ,Robert A.Dunne , ISBN: 978-0-471-74108-4, WILY-INTERSCIENCE, 2007.