CATEGORIZING SYSTEM CRITICALITY GUIDELINE FOR UTM HEALTH CENTRE

ALI ABDULWAHID MOHAMED

UNIVERSITI TEKNOLOGI MALAYSIA

CATEGORIZING SYSTEM CRITICALITY GUIDELINE FOR UTM HEALTH CENTRE

ALI ABDULWAHID MOHAMED

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

Faculty of Computing
Universiti Teknologi Malaysia

SEPTEMBER 2014

This project is dedicated to my beloved and respected parents, supervisor and my beautiful wife for their endless love, support and encouragement. Thank you for the moral support and guidance given throughout my academic life.

ACKNOWLEDGEMENT

In the name of Allah, Most Gracious, Most Merciful.

First and foremost, I must be thankful to ALLAH for making me possible to successfully finish this research study. I am deeply grateful to my Supervisor, **Dr. Siti Hajar Othman** for her exemplary guidance, encouragement, supports and honestly unforgettable efforts spent to my graduation project from the initial phases to the final phase have been extremely useful. I take this opportunity to express my deep gratitude to the lasting memory of my lovely parents, brothers, sisters and my beautiful wife without their patience, understanding, support and most of all love, the completion of my degree would not be successfully possible.

Finally, I would like to extremely grateful to Universiti Teknologi Malaysia (UTM) particularly Faculty of Computing (FK) for their best efforts to provide me all the educational facilities and support. It was an exciting study period in UTM and I feel privileged to have had the opportunity to carry out this study as a demonstration of knowledge gained during the period studying for this master degree. I would like to thank UTM Health Centre for their cooperation and time in helping me to provide information for the completion of this project. With these acknowledgments, i offer my regards and blessings to all of those who supported me in any respect during the completion of my degree including my colleague students and my instructors who contributed me their support and knowledge.

ABSTRACT

Categorization of system criticality is an approach of asset identification and classification regarding to the importance and the impact of its absence to the mission of the organization. Currently, many organization worldwide are heavily depend on different types of Information Technology (IT) to achieve their missions with efficient and effectively. Regarding to this unlimited use of technology, there are some problems which can directly or indirectly affecting various operations in the organization. Disasters are any occurrence that can cause an interruption of a critical organization's operations for unspecified period of time whereby the disasters effects can sometimes disrupt the organization completely. Categorization of system criticality guideline helps the organization to have a prepared rank for their organization's assets. Many organizations have tried to develop their own system criticality guideline but they do not have a systematic approach to follow. Therefore, this study will propose a categorization of system criticality guideline which is designed specifically for Universiti Teknologi Malaysia (UTM) Health Centre to be used as a guidance to categorize and prioritize their critical resources. The proposed guideline consists of nine (9) phases which include Understand the Organization and Analyze Process, Recognize Organizational Resources, Classify Systems and Functions, Identify Critical Resources and functions, Prioritize Critical Resources and Functions, Develop Recovery Time Strategies, Develop Responsibility Charts, Guideline Maintenance Process and Approve and Implementation. The proposed guideline was validated by three (3) experts through distributed-interview-questionnaire and the proposed guideline was improved regarding to their suggestions and recommendations.

ABSTRAK

Pengkategorian tahap sistem kritikal merupakan satu pendekatan pengenalan dan pengelasan aset berdasarkan kepentingan dan kesan kehilangannya kepada misi organisasi. Pada masa kini, setiap organisasi di dunia bergantung sepenuhnya kepada pelbagai jenis teknologi maklumat (IT) bagi memastikan misi mereka dapat dicapai dengan cekap dan berkesan. Mengenai penggunaannya yang menyeluruh, terdapat beberapa masalah yang secara langsung atau tidak langsung mengancam operasi organisasi. Bencana merupakan sebarang kejadian yang boleh menyebabkan gangguan operasi organisasi kritikal bagi tempoh yang tidak ditentukan di mana kesan bencana tersebut boleh menyebabkan organisasi lumpuh dengan serta-merta. Pengkategorian sistem secara kritikalnya mengariskan panduan untuk membantu organisasi menyediakan kategori bagi aset mereka. Terdapat pelbagai organisasi yang cuba untuk membangunkan garis panduan sistem kritikal mereka sendiri tetapi mereka tidak mempunyai pendekatan sistematik untuk diikuti. Dengan demikian, kajian ini akan mencadangkan pengkategorian garis panduan sistem kritikal yang direkabentuk khusus untuk Pusat Kesihatan Universiti Teknologi Malaysia (UTM) yang akan digunakan sebagai panduan untuk mengkategorikan dan mengutamakan sumber kritikal mereka. Garis panduan yang dicadangkan terdiri daripada sembilan (9) fasa yang terdiri daripada Memahami Organisasi dan Analisis Proses, Mengenali Sumber Organisasi, Sistem Mengklasifikasi dan Fungsi, Sumber Mengenalpasti Kritikal dan fungsi, keutamaan Sumber Kritikal dan Fungsi, Membangunkan Strategi Masa Pemulihan, Membangunkan Carta Tanggungjawab, Proses Garis Panduan Penyelenggaraan dan meluluskan dan Pelaksanaan. Garis panduan yang dicadangkan telah disahkan oleh tiga (3) orang pakar melalui temuramah dan soal selidik yang diedarkan dan hasilnya telah dipertingkatkan berdasarkan cadangan dan syor-syor mereka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BCP	-	Business Continuity Plan
BIA	-	Business Impact Analyze
C-I-A	-	Confidentiality, Integrity and Availability
CICT	-	Centre for Information Communication and Technology
DCRP	-	Disaster Contingency Recovery Plan
DRP	-	The Disaster Recovery Plan
HIRARC		Hazard Identification, Risk Assessment and Risk Control
HIS	-	Health Information System
MTD	-	Maximum Tolerable Downtime
OSHA		Occupational Safety and Health Act
RPO	-	Recovery Point Objective
RTO	-	Recovery Time Objective
WRT	-	Work Recovery Time

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

At the present time, most of the organizations that exist in the world transformed from paper data to digital data using advanced ways of storing their data to computer information systems which makes easier to done their business in sufficient and advanced manner while storing, reading, publishing, and also helps for decision making at the crucial situations (Chang, 2011a).

Since most of the healthcare organizations implemented an advanced and easy way of management towards their functional operations which is the implementation of Health Information System (HIS), the continuity and the stability of their system must be planned in order to be well successful. There are a lot of significant problems towards to every significant function inside the organization, especially to the information technology based systems within the healthcare centers. Regarding to the expensive healthcare information systems which are installed in the health centers, the need of system categorization and operational prioritizing to this useful system is absolutely required and important step to the right direction of organizational continuity (Heeks, 2006)

The revolution of computers and Internet facilities create the need of information systems that lead to any organization must benefit and utilize for the

well developed manner of storing gigabytes of data to a small device using computers. This is one of the reasons that every organization prefer to utilize this new technology because of the enhanced way of storing, communication and decision support.

There are two common terminologies which are usually related for the usage of computers. The first one is information technology which means using computer related technology that consists the combination of hardware and software applications in order to input data, process and store as information for later usage, and as well as communication technology for information transmission, at the other hand, information systems are integrated group of IT, procedures and the users who are responsible for the controlling, organizing and distribution of the information (Chang, 2011b).

Using information systems are increasing beyond our imagination. However, this revolution to digital world causes fears to the concept of information security (Confidentiality, Integrity, and Availability) which each of these concept is crucial to gain by any information system. Implementing information systems in health-based organization will facilitate and develop the way of the activities is done but their security become an important issue to be considered since the information system records of every patient is really very sensitive which needs extra attention of planning to prevent inconveniences and reduce losses (Smith and Eloff, 1999).

Emergency management and business continuity planning, which is when is combined together knows as contingency planning, is an important method to use for any organization that wants to survive and be successful for its mission functions. Contingency planning is not an easy task to do by any organization because it is a time consuming and very costly process, therefore, every organization whether a public or private establishes a different degree of contingency plans that depend on their abilities.

In the absence of proper and careful planning, when unexpected and catastrophic event happen to the organization will cause the loss of both people and critical asset. A lot of estimates declare the failure rates of the organizations after the disaster. Most of those failed organizations described that it was because of lack contingency planning and they suggest that preparedness will improve the organizations survival and minimize the degree of losses.

According to the fear of terrorist attacks, computer generated crimes, natural disasters, internal attacks, external attacks and their increasing costs, many organizations of both public and private are taking into account to develop contingency plans in order to help their people, assets, facilities and to continue their operations. As the organizations become more in size and the number of staff, the effect of the disasters can cause greater and more impacts than as usual, and that is the because of their huge staff and assets. Many proceeding actions that happen in the world such as the attack on the World Trade Center at New York in 2001, the Tsunami at Phuket in 2004 and the great destruction and damage left behind by Hurricanes Dennis, Emily, Katrina, Rita, and Wilma in 2005 have shown how these impacts can affect the entire world and wake up to many big organizations that previously unaware (Kerzner, 2002).

To effectively control business continuity for the duration of the unexpected event and bring back to the normal operations, every organization requires classification of their data. When the unexpected event happens, it is very important for the organizations to put together all their efforts and resources needed in order to continue their critical target operations. As experienced, time is very important and sometimes its value compared to money and in today's economy, an hour may have the value of thousands of dollars. Preparation before the unexpected event and categorizing the system according to their priorities to the organization will reduce the impact of the unexpected event (Al-Khabbaz et al., 2011).

Health-based organizations store useful information in their systems regarding to patients, therefore, categorizing system information according to the

criticality and priority of the stored information will help the organization for making rapid decision which part of the system will be recovered first after disaster occurs (Ide and Kaneta, 2004).

The most important objective of making recovery for the unexpected event is to assist the organization in the situation that may cause all or some parts of computer information system functions may become to unusable. Awareness of the unexpected event is an important factor that can help the organizations from being fall down, the planning process for the future should reduce the violation of operations and make sure some level of organizational strength and recovering mission-critical information systems (Wold, 2006).

Prioritizing information systems and functions for recovery is one of the most helpful activities that any organizations need to analyze before any interruptive event may happen and effect the normal situation of the organizational work follow. Asset criticality for health based organization is an important part for both managing and recovering the information system concerning to their cost, benefit and the impact to trust their information system and functions (Ide and Kaneta, 2004).

There are several guidelines and standards that are related how to develop a proactive plans in order to be implemented if any unexpected situations happen to organizations. However, Most of the guidelines are basically suitable for the big companies who are already official and have enough number of workers. While, the small and medium type of organizations who still do not have enough manpower and experts in this field, it will be difficult for them to follow the existing guidelines because of their complexity.

This project proposed a Categorizing System Criticality Guideline that specially can be used by small and medium type organizations. The case study for this project is Universiti Teknologi Malaysia (UTM) Health Centre. As a requirement from this organization, the Categorizing System Criticality Guideline should be a helpful for them to solve and reduce the impact of the disasters and

interruption problems. This means that the criticality guideline is completely necessary that will make the organization well organized and proactively planned.

1.2 Problem Background

Nowadays, most of the organizations that exist utilize information systems to facilitate their activities, the widely use of the information systems become one of the most critical asset to any particular organization. Due to the high value of information systems every organization must keep accurately and secure the confidentiality, integrity and availability of that expensive information. The fact is that, less care of this information will totally lead the destruction and prevent the continuation of the company process. Since the uses of information technology are greater than ever, the critical information of any organization become more valuable and are increasingly can be faced to many risk. To protect the organizations information, everyone in the organization should have their own responsibilities on securing the information including the top management or the board of director.

According to the criticality of information systems, Health-based organizations they also have a lot of valuable and sensitive information that are confidential concerning to the patient records. This information requires being perfect and should not to be viewed and altered by other parties except the individuals that have been authorized to do the changes. Without classification of data criticality the organizations will not success the security of their information and recovering from the damage.

Several existing organization in the world could not able to start again after a sudden events happen to them and that is because of luck of emergency plans and luck of system priorities to continue their operation. If these organizations were implemented some sort of mitigation for critical operation, surely they were able to limit the unexpected event into acceptable level. For the sake of their careless to

implement caused to totally finish their mission operations in one time. Not only careless but be for the sake of inexperienced in this field of planning in the future events.

With this high rate of failures, every organization needs to ensure that they are prepared to minimize the effects of all possible disasters and events that may happen to the organization. Many organizations have tried to have their own categorization of system criticality, but the issue is that they do not have a systemic guideline to develop for that. In fact, there is no specific standards exist for critical infrastructure protection (Theoharidou *et al.*, 2009). According to Dr. Isma'il B Ahmed director of UTM Health Centre a categorizing system criticality is very important to the organization in order to help the organization for the preparedness of the disasters. Therefore, it is essential to have a guideline for categorizing information criticality as the guidance for the organization to follow during emergencies.

1.3 Problem Statement

Many health-based organizations put their effort to protect their information system from any harm, damage, loss, stealing, etc. all of these problems may cause a big loss to the organization that may force them to stop their activities, in order to prevent such kind of damages every organization must spend over thousands to implement a strong security mechanism to protect their systems.

There is no common guideline for health-based organizations regarding to how to categorize health information systems according to the criticality, because every organization uses different guideline to minimize the impact of the disaster. However, health-based information systems are strongly in need a guideline for categorizing system criticality to ensure the continuity of the operations and prevent the damages of their assets after and before unexpected disaster happens.

However, due to the importance of information and resources in the UTM Health Centre, a categorizing system criticality guideline is very essential because an incident can happen at any time without any prior notification. Furthermore, the organization needs to have their own categorizing system criticality guideline that will guide the organization the way they prioritize and protect their sensitive information to make sure that nothing will affect organization assets. This guideline will help UTM Health Centre to ensure the balance between the information security goals triangle of Confidentiality, Integrity and Availability (C-I-A).

1.4 Project Aim

The aim of this study is to propose a categorizing system criticality guideline for UTM Health Centre; this preliminary guideline helps the organization to prepare and plan the continuity of their operations after unexpected situation happens.

1.5 Project Objective

The following are the main objectives of this project and the final result would be depending on the following objectives:

- To study and analyze existing categorizing system criticality guidelines to evaluate which guidelines is suitable to the organization.
- To propose a categorizing system criticality guidelines for UTM Health Centre.
- To validate the proposed categorizing system criticality guidelines, whether it suitable and meets the organization needs.

1.6 Project Scope

The scope of this project focuses on the development of categorizing system criticality guideline for UTM Health Centre to ensure the continuity of the operations after a disaster happens. This guideline will help for the organizations to be proactive in order to be reactive, because mitigation and prevention are always better than recovering.

1.7 Importance of the Project

This project is important for information storing systems especially UTM Health Centre organization in terms of:

- Developing effective and efficient guideline for categorizing and prioritizing system criticality.
- Controlling, protecting and enhancing the value of data and information assets within the information systems.
- Minimizing the possibility and impact of interruptions of disaster to the information systems.
- Developing a guideline for protection the critical information according to their significance in the health based organizations.

1.8 Organization of the Project

This project report consists of six chapters. Every chapter is organized accordingly to a different work that involved in the study. The description of each chapter will be discussed in the following paragraphs.

Chapter 1 is the fundamental part of this project which highlights a brief understanding about various sections such as the overview of the study, problem background, the problem statement, aim of the study, project objectives, project scope and importance of this project.

Chapter 2 of this report covers recent review of the literature review that related to the study area which is categorization and system criticality guideline, this chapter also covers the importance of emergency management, business continuity planning and the health care organizations during disasters. This chapter also will discuss the previous researcher work in scope security issues and its problem.

Chapter 3 explain the technique of method that will be used in the study and also the operational framework will be described phase by phase and in details that will represent the flow of all tasks in doing this research.

Chapter 4 will be discussed on the design of the guideline implementation process. It consists of the processes and the phases or the features been selected in order to develop a categorizing system criticality guidelines. Lastly, a categorizing system criticality will be presented to validate by the experts in this field of the study.

Chapter 5 will be discussed on analysis of the result findings based on the expert's feedback. The result of the validation process of the guidelines also explained in order to be finalized the result of the guideline design. The description and the discussion of the results are also explained in this chapter. Besides, the finalized of business continuity planning guideline is present in this chapter.

Chapter 6 is the final chapter which consists of discussion on the conclusion of the project. The main points that this chapter will be discussed are research achievement, challenge and constraint of doing the research and future

recommendation towards this research. Lastly conclusion of this research project will be all concluded in this chapter.

1.9 Summary

In summary, this chapter describes the overall understanding of this study such as introduction, problem background, problem statement, objectives, project scope, importance of the project and organization of the project. All information contained in this chapter will be used as input to all of the following chapters.

REFERENCES

Al-Khabbaz, F., Al-Zahir, H., Elwi, S. and Al-Yousef, H. 2011. Disaster recovery planning & methodology for Process Automation Systems. *Proceedings of the 2011 EUROCON - International Conference on Computer as a Tool (EUROCON), 2011 IEEE*. 27-29 April 2011. 1-4.

Avelar, V. 2007. Guidelines for Specifying Data Center Criticality/Tier Levels. *LAMDA HELLIX*.

Bishop, M. 2003. What is computer security? *Security & Privacy, IEEE*. 1(1), 67-69.

Cerullo, V. and Cerullo, M. J. 2004. Business continuity planning: a comprehensive approach. *Information Systems Management*. 21(3), 70-78.

Chang, P. H. 2011a. Modeling the Management of Electronic Health Records in Healthcare Information Systems. *Proceedings of the 2011a Cyber-Enabled Distributed Computing and Knowledge Discovery CyberC, 2011 International Conference on*. 10-12 Oct. 2011. 580-584.

Chang, P. H. 2011b. Modeling the management of electronic health records in healthcare information systems. *Proceedings of the 2011b*, 580-584.

Conrad, E., Misenar, S. and Feldman, J. 2010. Chapter 7 - Domain 6: Business continuity and disaster recovery planning. In Conrad, E., Misenar, S. & Feldman, J. (Eds.) *CISSP Study Guide* (pp. 211-254). Boston: Syngress.

Da Veiga, A. and Eloff, J. H. P. 2010. A framework and assessment instrument for information security culture. *Computers & Security*. 29(2), 196-207.

Davis, G. B. 2003. Management information systems (MIS).

Ellison, R. J., Fisher, D. A., Linger, R. C., Lipson, H. F., Longstaff, T. A. and Mead, N. R. 1999. Survivability: protecting your critical systems. *Internet Computing, IEEE*. 3(6), 55-63.

Erbschloe, M. 2010. *Guide to Disaster Recovery*. Thomson/Course Technology.

Firesmith, D. 2004. Prioritizing Requirements. *Journal of Object Technology*. 3(8), 35-48.

Fischer, R. J., Halibozek, E. P. and Walters, D. C. 2013. 11 - Contingency Planning, Fire Protection, Emergency Response and Safety. In Fischer, R. J., Halibozek, E. P. & Walters, D. C. (Eds.) *Introduction to Security (Ninth Edition)* (pp. 241-282). Boston: Butterworth-Heinemann.

Gantz, S. D. and Philpott, D. R. 2013. Chapter 15 - Contingency Planning. In Gantz, S. D. & Philpott, D. R. (Eds.) *FISMA and the Risk Management Framework* (pp. 403-443)Syngress.

Goolaup, T. M. F. M. P., Minol, E. K. E. T. K., Faalafi, M. K. S. P. S., Watson, L. B. C. S. C., Tovia, M. J. J. S. V., Joris, S. S. J. K. A., Mow, K. E. V. I. C., West, P., Williams, I. M. J. M. J. and Askounis, T. A. H. F. H. Introduction to Disaster Management.

Hammoum, H., Bouzelha, K., Ait Aider, H. and Hannachi, N. E. 2014. Tanks criticality assessment by the dependability method. Case study. *Engineering Failure Analysis*. 41, 10-22.

Heeks, R. 2006. Health information systems: Failure, success and improvisation. *International Journal of Medical Informatics*. 75(2), 125-137.

Ide, A. and Kaneta, N. 2004. A study on disaster management about the protection of spreading rumors on the network. *Proceedings of the 2004 Information and Communication Technologies: From Theory to Applications, 2004. Proceedings. 2004 International Conference on*. 19-23 April 2004. 25-26.

Ilvonen, I. 2013. Information security assessment of SMEs as coursework - learning information security management by doing. *Journal of Information Systems Education*. 24(1), 53-59.

Janczewski, L. and Xinli Shi, F. 2002. Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computers & Security*. 21(2), 172-192.

Kerzner, H. R. 2002. *Strategic planning for project management using a project management maturity model*. John Wiley & Sons.

Lindström, J., Samuelsson, S. and Hägerfors, A. 2010. Business continuity planning methodology. *Disaster Prevention and Management*. 19(2), 243-255.

McGill, W. L., Ayyub, B. M. and Kaminskiy, M. 2007. Risk analysis for critical asset protection. *Risk Analysis*. 27(5), 1265-1281.

Mead, N. R. and Stehney, T. 2005. *Security quality requirements engineering (SQUARE) methodology*. (Vol. 30)ACM.

Mohamed, M., Stankosky, M. and Mohamed, M. 2009. An empirical assessment of knowledge management criticality for sustainable development. *Journal of Knowledge Management*. 13(5), 271-286.

Moss, T. and Woodhouse, J. 1999. Criticality analysis revisited. *Quality and reliability engineering international*. 15(2), 117-121.

Nosal, R. and Schultz, T. 2008. PQLI definition of criticality. *Journal of Pharmaceutical Innovation*. 3(2), 69-78.

Oberg, J. C., Whitt, A. G. and Mills, R. M. 2011. Disasters will happen-are you ready? *Communications Magazine, IEEE*. 49(1), 36-42.

Peltier, T. R. 2013. *Information security fundamentals*. CRC Press.

Rogers, R., Miles, G., Fuller, E., Dykstra, T. and Hoagberg, M. 2004. Chapter 3 - Determining the Organization's Information Criticality. In Rogers, R., Miles, G., Fuller, E., Dykstra, T. & Hoagberg, M. (Eds.) *Security Assessment* (pp. 81-118). Burlington: Syngress.

Rushby, J. 1994. Critical system properties: survey and taxonomy. *Reliability Engineering & System Safety*. 43(2), 189-219.

Smith, E. and Eloff, J. H. P. 1999. Security in health-care information systems—current trends. *International Journal of Medical Informatics*. 54(1), 39-54.

Snedakar, S. 2007. Chapter 31 - Business Impact Analysis. In Snedakar, S. (Ed.) *The Best Damn IT Security Management Book Period* (pp. 733-771). Burlington: Syngress.

Theoharidou, M., Kotzanikolaou, P. and Gritzalis, D. 2009. Risk-based criticality analysis *Critical infrastructure protection III* (pp. 35-49)Springer.

Thompson, H. 2013. The human element of information security. *IEEE Security and Privacy*. 11(1), 32-35.

Torabi, S. A., Rezaei Soufi, H. and Sahebjamnia, N. 2014. A new framework for business impact analysis in business continuity management (with a case study). *Safety Science*. 68(0), 309-323.

Wold, G. H. 2006. Disaster recovery planning process. *Disaster Recovery Journal*. 5(1).