A VIRUS DISASTER RECOVERY PLAN FRAMEWORK FOR ACADEMIC COMPUTING CENTER

MOHAMED ISMAIL GURHAN

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

JANUARY 2014

Dedicated to my beloved mother, my father and my siblings

ACKNOWLEDGEMENT

I wish to express my deepest appreciation to all those who helped me in one way or another to complete this project. First and foremost I thank Allah almighty who provided me with strength, direction and purpose throughout the project. Special thanks to my project supervisor Dr. Norafida Bint Ithnin for all her patience, guidance and support during the execution of this project. Through his expert guidance, I was able to overcome all the obstacles that I encountered in these enduring seven months of my project. In fact she always gave me immense hope every time I consulted with her over problems relating to my project.

I take this opportunity to thank my friends for taking time out of their busy schedule to help me. Last, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as computer laboratory to complete this project.

ABSTRACT

This thesis presents a Virus disaster recovery plan framework for academic computing centre. The CICT-UTM is taken as case study. The proposed framework consists of seven phases of disaster recovery plan which has been enhanced in improved by researcher based on past studies. The phases of the framework are risk assessment, prevention, preparedness, reaction, immediate recovery, restoration and review. The type of disaster in this study focuses on virus threats. In addition, the framework describes the virus management process in each phases which is before, during and after virus occurs. The framework of virus disaster recovery plan outlined here should provide the dictionary necessary for planning any Academic Computing Centre. The project is a case study based with interviews, documentation and questionnaire as the key to improve virus disaster recovery plan and any similar organization to provide a knowledge feedback. An enhanced framework will be proposed that will be validated by an expert.

ABSTRAK

Tesis ini membahas tentang susunan pelan pemulihan bahaya virus untuk keperluan pusat akademik komputer. CICT dirujuk menjadi kasjian kes. Susunan yang diusulkan terdiri dari tujuh fasa pelan pemulihan yang mana telah dipertingkatkan menjadi lebih baik melalui penyelidikan terhadap kajian yang lepas. Fasa dari susunannya iaitu penilaian risiko, pencegahan, persiapan, tindak balas, pemulihan segera, pemulihan maklumat, dan ulasan. Jenis jenis dari bahaya virus dalam kajian ini bertumpu kepada ancaman virus. Di samping itu, susunan kerja ini menerangkan tentang proses pengurusan virus di tiap fasa sebelum, semasa, dan selepas virus menjangkiti. Susunan kerja pelan pemulihan virus yang diuraikan pada kajian ini menyediakan kamus yang diperlukan untuk perencanaan pusat akademik maklumat. Proyek ini merupakan kajian kes yang berbasis kepada wawancara, dokumentasi dan kuisioner sebagai kunci untuk membaiki pelan pemulihan bahaya virus dan organisasi yang serupa untuk memberikan rekomendasi. Susunan kerja akan diajukan dan disahkan oleh seorang pakar.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBRIVIATIONS

ACC	-	Academic Computing Centre
CERT	-	Computer Emergency Response Team
CSI	-	Computer Security Institute
DMZ	-	Demilitarized Zone
EDI	-	Electronic Data Interchange
ICT	-	Information Communication and Technology
IDC	-	International Data Centre
IMSS	-	InterScan Messaging Centre
ISLAN	-	Integrated Sintok Local Area Network
ISO	-	International Standards Organization
IT	-	Information Technology
LAN	-	Local Area Network
LE	-	Local Environment
LN	-	Local Network
MANPU	-	Malaysian Administrative Modernization and Management Planning Unit
MOU	-	Memorandum Of Understanding
MYCERT	-	Malaysian Computer Emergency Response Team
MYMIS	-	Malaysian Public Sector ICT Management Security Handbook
NCSA	-	National Computer Security Association
NISER	-	National Institute and Emergency Response Centre
NIST	-	Institute of Standards and Technology
POE	-	Panel and Expert
UTM	-	University Technology Malaysia
VLAN	-	Virtual LAN
WAN	-	Wide Area Network

CHAPTER 1

INTRODUCTION

1.1 Overview

Disaster recovery planning is a topic which has received recently increasing attention in recently issue of computer-related publications. Growing number of organizations are become aware of the need for such planning. Disaster recovery plan is crucial component used to ensure systems that are critical to the operation of the organization, are available when needed (Tipot and Krause 2010). After all the main purpose of disaster recovery plan (DRP) is to allow an organization to recover in case of an unexpected event.

Disaster can strike many times, and the best way to handle it is to be prepared. Many do not realize the importance of the DRP. Often, it takes catastrophic event to propel organizations to consider more rigorous disaster recovery plan, Ferrarini (2008). This statement also supported by Hawkins et al.(2008) that claimed most organization hesitates to develop a DRP until a disaster occurs. As claimed by Adshed (2008), only six percent of firms in United Kingdom have disaster recovery plans.

As examples the recent major power outage that paralysed the north east-east of united of united states and Canada on late evening August 14, 2003, Zahri and Li

(2008). It has created uncertain and challenging environment specially for most organizations there. In addition, the occurrence disrupts the functioning of the organization resulting in loss of data of business or loss of time. Furthermore, the tragic event of September 11, 2001 makes organizations take a fresh look at their disaster plans (Sybase, 2003). The events made disaster recovery planning rise to the top of every organization's information technology department in their priority list. It has provided a wakeup call and most organization become aware on the importance of DRP.

Risk and uncertainties are part of the everyday operating environment for all organizations. According to Davies and Walters (2003), the risk may be sufficient to generate a crisis, which if left unattended, can become a disaster. In essence, a disaster includes any type of interruption of service that rules from some force beyond the organization's control. Disaster can come in many types; the best thing is to be well prepared. A virus attack is an example of disaster. Virus can only survive in a computer system or systems such as a network. According to incident statistics provided by Malaysian Computer Emergency Response Team (MyCERT), and National ICT Security and Emergency Response Centre (NICER), in year 2009there were 27 incidents of virus threats reported occurred in Malaysia. The flowing year showed disturbing numbers which incidents of a virus attack soaring to 379 cases. Then in year 20010 he report on major virus outbreaks showed the figures increase to 514 cases. Currently, in January 20011 there were 26 incidents has been reported, subsequently in February showed the numbers decline to 23 incidents and finally in March, the incidents boost up to 42 cases of virus attack (MyCERT and NISER, 2010).

1.2 Problem background

Growing numbers of organization are become aware of need such planning. Disaster recovery plan is crucial components used to ensure systems that are critical to the operations of the organization are available when needed. After all the main purpose of a disaster recovery plans to allow an organization to recover in case of an expected event.

Disaster can strike anytime, and the best way to handle it to be prepared. Many do not realize the importance of disaster recovery plan. it takes catastrophic event to propel organizations to consider more rigorous disaster recovery plan , most organizations hesitate to develop a Disaster recovery plan until a disaster occurs . in addition to that the occurrence disrupts the functioning of the organization resulting in loss of data loss of business and loss of time . Furthermore the target events of September 11, 2011 make organizations taken a fresh look at their disaster plan .

The serious of virus is evidence by Microsoft's effort to capture the virus writer. As example Microsoft has issued considerable reward for information leading to the successful conviction of a virus writer in the past. In februery 2010, the company offered 250,00 dollars for the capture of the MyDOOM worm author, and last year a total of half a million dollars concerning the Sobig-F and Blaster worms (Sophos,2010). Recently variants of the sasser worm have been found in several countries throughout Europe, Asia, Latin America and the United States. It has already four variants, which takes advantage of the Microsoft vulnerability, the effect windows 2000, windows ME, windows XP, windows95 and 98 platforms (Maneksha, 2008). Security software and services provider, Trend Micro Inc. ranks the seriousness of the Sasser.B variant as the highest in terms of the severity, thus warning a red alert, (Wong,2008) said Sasster is network virus which is different from application virus that infects e-mails. Anyone connected to the internet, including corporate networks and broadband subscribers, may at the risk from the family of worms. Besides the trend over the last few years has seen changes in virus

attacks especially in terms of its behaviour, speed of the spreading and the way it spreads.

1.3 Problem Statement

In every organization computer centre flows basic guidelines on disaster recovery documents provided by Malaysian administrative modernization and management planning unit. so one of the agency's role is responsible in providing basic guideline which can be flowed by other public sector.so the document which have brief elements, is :- MYMIS(the Malaysian public sector ICT management security handbook).

More documents including this are a broad circular which simply stated that systems must recover from any disruptions to insure its availability and accessibility in other to minimize loss. It suggests organization should formulate and test its own disaster recovery plan, implement data back up and apply good practices of ICT.

Meanwhile, MyMIS handbook provides the general guidelines on ICT security management safeguards to enable implementation of minimal security measures. it only covered the disaster recovery and contingency planning checklist for ICT systems which consists of items for prevention and preparation , risk and resource assessment , test , evaluation and update the plan, and recover and restoration .

The document intended to address all possible ICT situations regardless the organization's background. They have no sufficiently covered on virus disaster recovery plan (DRP) or highlight in detail on specific disaster encountered such as a virus attacks which pertinent to an academic computing centre.

As result of these limitations, I propose a Virus disaster recovery plan framework, which focuses on virus attack in academic computing centre (ACC). The framework consists of virus management process in each face of the frame work.

In addition, on 2011, an accident of a virus attack has paralyzed the communication network in every department of an organization the disruptions caused by virus which made the whole email systems and internet an available and inaccessible. An accident of a virus which capable to open a backdoor on infected systems allows malicious hackers to run unauthorized code and launch a denial of services attack on Microsoft's website occurred worldwide.

The examples of above, those incidents classified as a critical problem of a virus attack in a network. If organization is unprepared before, during and after disaster, the impact is unimaginable. Therefore this project is attempts to address on disaster recovery plan, which put emphasis on a virus threats in network setting purposely for academic computing centre (ACC).

1.4 Objectives of the Project

To analyse the existing problems in the CICT-UTM network that my Cause a disaster

- To propose framework to overcome those problems focusing on virus threats
- To validate the framework

1.5 Scopes of the Project

This research will focus on academic computing centre CICT in University Technology Malaysia as a case study the efforts highlight on providing a disaster recovery framework for computer disaster, which is attack of a virus in the network settings. It will point up the virus management process that I will mention each face of the framework. There will be some questions that I will attempt to answer in the project questions which are:

What is the available virus disaster recovery plan framework for academic computing centre CICT?

What is the suitable virus disaster recovery plan framework that focuses on virus threat for academic computing centre?

1.6 significance of study

The research shows the importance of DRP in an academic computing centre environment. The disaster recovery framework will facilitate UTM computer centre in preparing and preventing for virus attack in network setting by implementing actions to avoid and lessen its impact. The DRP framework is able to help as guidance to prepare, prevent and reducing disruptions to organization operations. As the virus management processes are designed and organized appropriately before , during and after disaster; UTM computing centre operations can be re-established quickly with minimal delays this agreed by Bates (2010),which claimed disaster recovery planning could help organization recovery from a disaster quickly. Besides, Hawkins et al.,(2009) also admit the proposed disaster recovery framework my help an orderly recovery for organization. It covers most of the problems that could happen during the virus attack and it provides necessary resources to solve those

problems. Finally, this research contributes a DRP framework, which aims at virus threat the network for academic computing centre. Besides, the organized virus management processes in each phase in the framework can be used as a main guideline in handling virus attack.

REFRENCES

Arnel. Interviews An Introduction to Qualitative Research Interviewing, Sage Publications, 200

Baldwin, A. et al., 2006. A model-based approach to trust, security and assurance. , 24(4).

Bartolini, C., Stefanelli, C. & Tortonesi, M., 2010. SYMIAN : Analysis and Performance Improvement of the IT Incident Management Process. , 7(3), pp.132-144.

Chantico Publishing Company Inc., 2006 How to use qualitative methods in evaluation. Newbury Park, CA: Sage, printer publication, New York, 10010.

Edwards, Z., Xi, G. & Jinming, C., 2009. Research on Architecture and Key Technology of Information Security virus effect . , pp.1-4.

Goh, M.H. 2008. Developing a suitable business continuity planning methodology.

Information management and computer security ,4(2), 11-13

Hawkins, S., David, C,Y., &DAVID CC,2009. Disaster recovery planning : a strategy for data security information management and computer science ,

Heikinen, D., &sarkis ,J 2006. Disaster recovery issues for EDI systems. Logistics information management

Hendrix, T.D., & Schneider, M.P. 2010 NASA's TReK project: a case study in using the spiral model of software development. Communication of the ACM, 45(4),152-159

Hopkins, K. 2009 ensuring network security retrived april 21, 2010 from http:/www.bussinessweek.com /adsections/2009/pdf/0350security.pdf

Hubbard ,J.C.,& Forcht, K.A. 2008.computer virus , how campanies can protect their systems. Industrial management &data systems , 98(1) 12-16.

hyperDictionary. 2010. framework: dictionary entry and meaning Retrieved May 1, 2013, fro http:/hayprerdictionary.com/dictionary/framework.

Hwkins , A., Hadgkiss, J. & Ruighaver, A.B., 2012. AC SC. Computers & Security. Available at: http://dx.doi.org/10.1016/j.cose.2012.04.001.

Hazards XVIII, 2004, IChemE Symposium Series No 150, Process Safety—Sharing Best Practice, pp. 652–725 (IChemE). HSG48, 1999, Reducing Error and Influencing Behaviour, p. 12 (HSE Books).

Hiatt, S., 2011. Disaster Recovery Journal 2011 IEEE/IPSJ International Symposium on Applications and the Internet, pp.352-352. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6004184 [Accessed May 8, 2013].

Ibrahim M.S. Fakharul –razi A. & S'ari M 2006 technological disaster criteria and models Disaster prevention and management, 12 (4), 305-311.

Job, M., 1998, Air Disasters Volume 3 (Aerospace Publications Pty). N Kariuki, G. and Lo¨we, K., 2004, Incorporation of Human Factors in the Design Process, guide prepared for PRSIM Focus Group 4, Institute for Plant and Process Technology, Process Safety and Plant Technology, Technische Universita¨t Berlin, Germany. Available from World Wide Web: http://www.prism-network.org/, accessed January 2005.

Kletz, T., 1999, HAZOP and HAZAN Identifying and Assessing Process Industry Hazards, p. 158 (IChemE).

Kakoli 2004. Structuring Incident Types to Streamline Incident Response. 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks, pp.456-462. Available at:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6117465 [Accessed May 8, 2012].

Kletz, T., 2004, Trevor's Corner, Previous Issues, Corner no 1 Available from World Wide Web: http://psc.tamu.edu/TrevorSays/T%27s%

LI,. 2008, HAZOP and HAZAN Identifying and Assessing Process Industry Hazards, p. 158 (IChemE

20corner%201%20Rev.pdf, accessed January 2005 from Mary Kay O'Connor Process Safety Center, http://psc.tamu.edu. Out of Control 2003, 2nd edition, pp. 44–45 (HSE Books).

MAMPU. 2006 the Malaysian public sector ICT management security handbook. From http:/www.manpu.gov.my/ict/MyMIS/chapter3.PDF

MyCERT & NISER. 2008.incidents statistics. Retrieved may 2 ,2013, from http://www.mycert.org.my/

MyCERT. 2004. Situational report and major worms outbreaks up to year 2003 in Malaysia Retrieved May 1,2013, from http://www.mycert.org.my/other _ recourses/NICER-MYC-PAP-7070-1.PDF

Maneksha,, Sarriegi, Jose Mari & Gonzalez, J.J., 2008. Incident Response and User Awareness. , pp.161-172.

Nem, 2010. A Context for Information Systems Security Planning. , 7, pp.455-465.

Polk , N.B. et al., 2010. An investigation and survey of response options for disaster recovery (virus).

Reese , P., 2011. Structuring virus Types to Streamline business continuity . 2011 Seventh International Conference on Mobile Ad-hoc and Sensor Networks, pp.456-462. Available at:

http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6117465

Raha 2004. & Jinming, C., 2009. Research on Architecture and Key Technology of Information Security Emergency Response. , pp.1-4.

Reese 2007 G. B. White, E. A. Fisch, and U. W. Pooch, "Cooperating security managers: A peer based intrusion detection system," IEEE Network, vol. 10, pp. 20-23, 1996.

Shenton, Z., Research on The Key Techniques of Wireless Communication for Emergency Information System. , pp.432-435.

Swanson, S. & Wang, W., 2010. A Campus Network Security –virus prevention Technical System Based on Emergency Log. , pp.3-5.

Toigo, Z., Research on The Key Techniques of Wireless Communication for Emergency Information System according virus attack. , pp.432-435.

Wong, , J.P., 2008. Establishing a Computer Security virus disaster recovery (VDR) NIST Special Publication 800-3.

Yiu and Tse as cited in Ruslan 2009. A Campus Network Security Emergency Response Technical System Based on Emergency Log. , pp.3-5.