A NETWORK DISASTER RECOVERY PLAN FRAMEWORK FOR ACADEMIC COMPUTING CENTRE

ADIBAH CHE MAT DAON

UNIVERSITI UTARA MALAYSIA
2004

A NETWORK DISASTER RECOVERY PLAN FRAMEWORK FOR ACADEMIC COMPUTING CENTRE

A thesis submitted to the Graduate School in partial
Fulfillment of the requirements for the degree
Master of Science (Information Technology)
Universiti Utara Malaysia

By
Adibah Che Mat Daon

JABATAN HAL EHWAL AKADEMIK
(*Department of Academic Affairs*)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

ADIBAH CHE MAT DAON

calon untuk Ijazah
(candidate for the degree of) **MSc. (IT)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/ her project paper of the following title)

A NETWORK DISASTER RECOVERY PLAN FRAMEWORK FOR ACADEMIC COMPUTING CENTER

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the filed is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **MRS. NAFISHAH OTHMAN**

Tandatangan
(Signature) : 

Tarikh
(Date) : 23/6/04

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or, in their absence, by the Dean of the Graduate School. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of material in this thesis, in whole or in part, should be addressed to:

Dean of Graduate School
Universiti Utara Malaysia
06010 UUM Sintok
Kedah Darul Aman.

ABSTRAK

Tesis ini memaparkan kerangka kerja bagi pelan pemulihan bencana rangkaian untuk pusat komputer universiti. Universiti Utara Malaysia dijadikan sebagai kajian kes. Cadangan kerangka kerja pelan pemulihan bencana ini mengandungi tujuh fasa yang telah ditambah baik dan diperkayakan oleh pengkaji berdasarkan kajian-kajian yang lepas. Fasa-fasa di dalam kerangka kerja in adalah penilaian risiko, pencegahan, penyediaan, tindakan, pemulihan segera, pengembalian, dan pemeriksaan semula. Jenis bencana yang difokus di dalam kajian ini ialah ancaman virus. Tambahan lagi, kerangka kerja ini menggambarkan proses pengurusan virus bagi setiap fasa yang merangkumi sebelum, semasa dan selepas serangan virus. Kerangka kerja bagi pelan pemulihan bencana rangkaian yang dipaparkan sewajarnya menyediakan hala tuju perancangan untuk mana-mana pusat komputer universiti.

ABSTRACT

This thesis presents a network disaster recovery plan (DRP) framework for academic computing centre. Universiti Utara Malaysia Computer Centre is taken as a case study. The proposed framework consists of seven phases of disaster recovery plan which has been enhanced and 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 processes in each phases which is before, during and after virus occurs. The framework of network disaster recovery plan outlined here should provide the direction necessary for planning at any academic computing centre.

ACKNOWLEDGEMENTS

I would be forever grateful to several individuals who have helped to shape my perspective on this study. First and foremost, my supervisor, Mrs. Nafishah Othman, who has provided special guidance, continued faith and support. Without her guidance, I would have pursued a number of dead-end streets.

Mr. Azman Ta'a, AP Hatim, Mr. Rizalman, Mr. Salleh Huddin, Mrs. Roslina, Mr. Amri, AP Bashah, and Mrs. Zahurin deserve special mention. They have supplied thoughts, advices, challenges, criticism and suggestions that have influenced my thesis writing.

Heartfelt thanks also go to my beloved family, for their prayers and constant support, morally and financially. Thanks dad (Che Mat Daon), mom (Aishah), sisters (Bazliah, Adilah, Nasyitah and Adlina), brothers in law (Zuhori and Hafiz) and my nephew (Farhan).

And, last but never least I would like to thank to my friends, Mon, Zack, Zura, Cik Dah, Bad, Umi, Norli, Mek Na, Wani, Kak Yati, and Wati for their support and advice. Their assistance has been a great compromise for the accomplishment of my study.

I apologize if I have forgotten to mention someone else; the oversight is accidental. Thank to you all, great and wonderful persons.

Last but not least, my utmost thanks and gratitude to God for giving me the courage to persevere with high dedication till the accomplishment of my Masters Degree study.

TABLE OF CONTENTS

	Page
PERMISSION TO USE	I
ABSTRAK	II
ABSTRACT	III
ACKNOWLEDGEMENTS	IV
TABLE OF CONTENTS	V
LIST OF TABLES	IX
LIST OF FIGURES	X
LIST OF ABBREVIATIONS	XI
CHAPTER ONE: INTRODUCTION	1
1.1 Problem Statements	4
1.2 Research Objectives	6
1.3 Scope of Study	6
1.4 Significance of the Study	7
1.5 Thesis Structure	8
CHAPTER TWO: LITERATURE REVIEW	9
2.1 UUM Computer Centre Background	9
2.1.1 Objectives and Roles	10
2.1.2 Application's System	11
2.1.3 Network Security	11
2.2 What Is A Disaster?	13
2.2.1 Virus: A Disaster in an Academic Computing Centre	15
2.2.2 Virus Overview	19
2.2.3 Characteristics of a Virus	21
2.2.4 Virus and Network Overview	22

2.2.5 The Impact of the Viruses 25
2.3 Disaster Recovery Plan (DRP) 27
2.3.1 What is Disaster Recovery Plan (DRP)? 29
2.3.2 Benefits of Disaster Recovery Plan 31
2.3.3 Disaster Recovery Plan Challenges 32
2.4 Previous Studies 35
2.4.1 Previous Study 1 36
2.4.2 Previous Study 2 37
2.4.3 Previous Study 3 38
2.4.4 Previous Study 4 39
2.4.5 Previous Study 5 41
2.4.6 Previous Study 6 42
2.5 Chapter Conclusion 43

CHAPTER THREE: METHODOLOGY 44
3.1 Spiral Model 44
3.2 Spiral Model for Network Disaster Recovery Plan Framework 45
3.2.1 Phase 1: Planning 46
3.2.2 Phase 2: Studies 47
3.2.2.1 Internet Search 48
3.2.2.2 Interview 49
3.2.2.3 Literature Search 50
3.2.3 Phase 3: Formulate 55
3.2.4 Phase 4: Expert Review 58
3.3 Chapter Conclusion 60

CHAPTER FOUR: RESULTS AND FINDINGS 62
4.1 Findings: A Network Disaster Recovery Plan (DRP) 62
Framework for Academic Computing Centre

4.1.1 Phase 1: Risk Assessment 65
4.1.2 Phase 2: Prevention 70
4.1.2.1 Antivirus Software Deployment Points 72
4.1.2.1.1 The Desktop-Based Solution 74
4.1.2.1.2 The Server-Based Solution 74
4.1.2.1.3 Internet Gateway Solution 76
4.1.2.2 Security Policy 76
4.1.2.2.1 Anti-virus Policy 77
4.1.2.3 Backup 79
4.1.2.4 Education and Awareness 80
4.1.3 Phase 3: Preparedness 83
4.1.4 Phase 4: Reaction 85
4.1.4.1 Detection 86
4.1.4.2 Form Centralized Operation Centre 88
4.1.4.3 Investigation 89
4.1.4.4 Disseminate Warning 89
4.1.4.5 Arrangements 90
4.1.5 Phase 5: Immediate Recovery 91
4.1.5.1 Isolate and Containment 92
4.1.5.2 Scan 94
4.1.5.3 Eradication 94
4.1.5.4 Recover and Prevention 95
4.1.5.5 Verification 95
4.1.6: Phase 6: Restoration 96
4.1.6.1 Reconnect and Restore 98
4.1.6.2 Monitoring 98
4.1.7 Phase 7: Review 99
4.1.7.1 Inspect 101
4.1.7.2 Report 103
4.1.7.3 Recommend and Update 103
4.2 Chapter Conclusion 106

CHAPTER FIVE: RECOMMENDATIONS AND CONCLUSIONS 107

5.1 Recommendations 107

5.1.1 Testing the Plan 108

5.1.2 Training 109

5.1.3 Management's Commitment 110

5.2 Future Research 110

5.3 Conclusion 111

REFERENCES 113

APPENDICES 121

LIST OF TABLES

	Page
Table 2.1: The impact of five major viruses and worms to the network	26
Table 2.2: Comparative study on cost caused by viruses	27
Table 3.1: Related work on disaster recovery plan obtained from previous studies	50
Table 3.2: Weaknesses and limitations of disaster recovery plan in previous studies	53
Table 4.1: Vulnerabilities that virus is most likely to exploit	66
Table 4.2: Summary of risk assessment phase	70
Table 4.3: Recommendations on users' education and awareness	81
Table 4.4: Summary of prevention phase	82
Table 4.5: Summary of preparedness phase	84
Table 4.6: Sign of virus	88
Table 4.7: Summary of reaction phase	91
Table 4.8: Containment strategies	94
Table 4.9: Summary of immediate recovery phase	96
Table 4.10: Summary of restoration phase	99
Table 4.11: Questions in post mortem and lesson learned meetings	102
Table 4.12: Summary of review phase	104

LIST OF FIGURES

	Page
Figure 2.1: Network security architecture	12
Figure 2.2: Virus incidents from January until December 2003	17
Figure 2.3: Virus incidents from January until March 2004	17
Figure 2.4: The most top ten virus attack on PC and network in UUM (until May 19, 2004)	19
Figure 2.5: Effects of viruses	25
Figure 2.6: Major security hurdles	34
Figure 3.1: Method used to meet the research objectives	46
Figure 3.2: The proposed network disaster recovery plan framework for academic computing centre	57
Figure 4.1: A network disaster recovery plan framework for academic computing centre	64
Figure 4.2: The virus management processes in risk assessment phase	69
Figure 4.3: Effective Internet computer virus protection policy	71
Figure 4.4: Virus prevention measures in prevention phase	73
Figure 4.5: The all entryways solutions (Internet firewall + server based antivirus + desktop based antivirus)	75
Figure 4.6: Disaster document plan in preparedness phase	85
Figure 4.7: The virus management processes in reaction phase	87
Figure 4.8: The virus management processes in immediate recovery phase	93
Figure 4.9: The virus management processes in restoration phase	97
Figure 4.10: The virus management processes in review phase	101
Figure 4.11: The review phase assess the weaknesses in the previous phase	105

LIST OF ABBREVIATIONS

ASIS	Academic and Record Student Information System
CERT	Computer Emergency Response Team
CLIMAS	Clinical Administration System
CSI	Computer Security Institute
DMZ	DeMilitirized Zone
DRP	Disaster Recovery Plan
EDI	Electronic Data Interchange
ES	End System
FBI	Federal Bureau of Investigation
GAIS	Graduates Academic Information System
ICSA	International Computer Security Association
ICT	Information Communication and Technology
IDC	International Data Centre
IFAS	Financial and Accounting System
IMSS	InterScan Messaging Secure System
ISLAN	Integrated Sintok Local Area Network
ISO	International Standards Organization
IT	Information Technology
ITS	Information Technology Services
LAN	Local Area Network
LE	Local Environment
LINTAS	Library Information System

LN	Local Network
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MOU	Memorandum of Understanding
MyCERT	Malaysian Computer Emergency Response Team
MyMIS	The Malaysian Public Sector ICT Management Security Handbook
NCSA	National Computer Security Association
NISER	National ICT Security and Emergency Response Centre
NIST	National Institute of Standards and Technology
PERSIS	Personnel Information System
PoE	Panel of Expert
PRAKTIKUM	Student Practicum System
PRISM	Chancellery Information System
ReCIS	Research and Consultation Information System
R&D	Research and Development
RS	Relay System
SAIS	Student Affairs Information System
SELAMAT	Security Department Information System
SPS	Spam Prevention Solution
UUM	Universiti Utara Malaysia
VLAN	Virtual LAN
WAN	Wide Area Network

CHAPTER 1

INTRODUCTION

Disaster recovery planning is a topic, which has received increasing attention in recent issues of computer-related publications. Growing numbers of organizations are becoming aware of the need for such planning. Disaster recovery plan is crucial components used to ensure systems that are critical to the operation of the organization, are available when needed (Tipton and Krause, 2000). After all, the main purpose of a disaster recovery plan (DRP) is to allow an organization to recover in case of an unexpected event.

Disaster can strike anytime, and the best way to handle it to be prepared. Many do not realize the importance of DRP. Too often, it takes catastrophic event to propel organizations to consider more rigorous disaster recovery plans (Ferrarini, 2001). This statement also supported by Hawkins *et al.*, (2001) that claimed most organization hesitates to develop a DRP until a disaster occurs. As claimed by Adshead (2003), only sixty percent of firms in United Kingdom have disaster recovery plans. As examples, the recent major power outage that paralyzed the north-east of the United States and Canada on late evening of August 14, 2003 (Zahri and Ahmad, 2003). It has created uncertain and challenging environment especially for most organizations there. In addition, the

The contents of the thesis is for internal user only

REFERENCES

Adshead, A. (2003, September). Only 60% of firms have disaster recovery plans. *Computer Weekly*, p.6.

Ahmad, N.M.Z., & Zahri, Y. (2004). *Computer virus: future cyber weapons.* Retrieved April 4, 2004, from http://www.niser.org.my/resources/computer_virus.pdf

Arnell, A. (1990). *Handbook of effective disaster/recovery planning.* New York: McGraw-Hill Publishing.

Bates, R.J. (1992). *Disaster recovery planning: networks, telecommunications, and data communications.* New York: McGraw-Hill, Inc.

Belfast Institute and North West Institute of Further and Higher Education. (2002). *Guidance on developing and maintaining computer disaster recovery plans in further and higher education.* Retrieved April 10, 2004, from http://www.rsc-ni.ac.uk/technical/Disrec.pdf

Boehm, B.W. (1988, May). A spiral model of software development and enhancement. IEEE Computer, pp. 61-72.

Boehm, B.W., Egyed, A., Kwan, J., Port, D., Shah, A., & Madachy, R. (1998). *Using the WinWin spiral model: a case study.* Retrieved April 4, 2004, from http://sunset.usc.edu/publications/TECHRPTS/1998/usccse98-512/usccse98-512.pdf

Boehm, B.W., & Hansen, W.J. (2001). *Understanding the spiral model as a tool for evolutionary acquisition.* Retrieved May 2, 2004, from http://www.software-engineer.org/downloads/Spiral%20Model%20as%20a%20Tool%20for%20Evolutionary%20Acquisition.pdf

Bruce, G., & Dempsey, R. (1997). *Security in distributed computing: did you lock the door?* New Jersey: Prentice Hall PTR.

Center for Technology in Government. (2003). *A survey of system development process model.* Retrieved April 4, 2004, from http://www.ctg.albany.edu/publications/reports/survey_of_sysdev?chapter=9&PrintVersion=2

Chantico Publishing Company, Inc. (1991). *Disaster recovery handbook.* United States of America: TAB Professional and Reference Books.

Cobb, C. (2003). *Network security for dummies.* New York: Wiley Publishing.

Cohn, E.R., Klinzing, G., Frieze, I.H., Sereika, S.M., Stone, C.A., Vana, C.M. (2004). Academic computing vulnerabilities: another view of the roof. Educause Quarterly, pp. 57-61.

Comprehensive Consulting Solutions, Inc. (2001). *Define what types of disasters that need to be planned for.* Retrieved April 10, from 2004, http://www.comp-soln.com/DRP2_whitepaper.pdf

Connor, D. (2003, September). Disaster-recovery plans still need work. *NetworkWorld,* p. 8.

Cooley, A. (2003). *Virus protection strategies to combat electronic attacks.* Retrieved May 19, 2004, from http://www.astaro.com/data/pdf/whitepapers/Whitepaper_VirusProtection_en.pdf

Coulthard, A., & Vuori, T.A. (2002). Computer viruses: a quantitative analysis. *Logistics Information Management, 15* (5/6), 400-409.

Data Management and Communications. (2003). *System engineering approach.* Retrieved April 4, 2004, from http://dmac.ocean.us/dacsc/docs/dmac_partIII_app5_9_30_03.pdf

Davies, H., & Walters, M. (1998). Do all crises have to become disasters? Risk and risk mitigation. *Property Management, 16* (1), 5-9.

Davis, K. (2001). Saving users from themselves: creating an effective student-oriented anti-virus intervention. *Proceedings of the SIGUCCS, USA,* 27-32.

Disaster Recovery Journal. (2004). *Business continuity glossary.* Retrieved March 11, 2004, from http://www.drj.com/glossary/DRJ-Glossary.pdf

Dix, A., Finlay, J., Abowd, G., and Beale, R. (1998). *Human-Computer Interaction.* 2nd Edition, Hertfordshire: Prentice Hall.

Eden and Matthews. (1996). Disaster management in libraries. *Library Management, 17* (3), 5-12.

Edwards, B. (1994). Developing a successful network disaster recovery plan. *Information Management & Computer Security, 2* (3), 37-42.

Edwards, B, and Cooper, J. (1995). Testing the disaster recovery plan. *Information Management & Computer Security, 3* (1), 21-27.

Eklund, B. (2001, December). Multi-faceted "continuity" plans are replacing simple data-recovery services in the wake of September 11. *Business Unusual,* pp. 20-25.

Ernst & Young. (1996). The Ernst & Young International Information Security Survey 1995. *Information Management & Computer Security, 4* (4), 26-33.

Farrokh, M. (2002). Evaluation and selection of an antivirus and content filtering software. *Information Management and Computer Security, 10* (1), 28-32.

Ferrarini, E.M. (2001). *How to create a disaster recovery plan before trouble strikes.* Retrieved March 28, 2004, from http://www.naspa.com/PDF/2001/1201%20PDF/70112006.pdf

Fites, P., Johnston, P., & Kratz, M. (1992). *The computer virus crisis.* New York: Van Nostrand Reinhold.

Fites, P.E., & Kratz, M.P.J. (1993). *Information systems security: a practitioner's reference.* New York: Van Nostrand Reinhold.

Furnell, S. M., & Warren, M.J. (1997). Computer abuse: vandalizing the information society. *Electronic Networking Applications and Policy, 7* (1), 61-66.

Goh, M.H. (1996). Developing a suitable business continuity planning methodology. *Information Management & Computer Security, 4*(2), 11-13.

Grance, T., Kent, K., & Kim, B. (2004). *Computer security incident handling guide: recommendations of the National Institute of Standards and Technology.* Retrieved May 19, 2004, from http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

Hannaford, C.S. (1995). Can computer security really make a difference? *Managerial Auditing Journal, 10* (5), 10-15.

Hawkins, S.M., David, C.Y., & David, C.C. (2000). Disaster recovery planning: a strategy for data security. *Information Management & Computer Security, 8* (5), 222-229.

Heikkinen, D., & Sarkis, J. (1996). Disaster recovery issues for EDI systems. *Logistics Information Management, 9* (6), 27-34.

Hendrix, T.D., & Schneider, M.P. (2002). NASA's TReK project: a case study in using the spiral model of software development. *Communications of the ACM, 45* (4), 152-159.

Hiatt, C.J. (2000). *A primer for disaster recovery planning in an IT environment.* Hershey: Idea Group Publishing.

Hopkins, K. (2003). *Ensuring network security.* Retrieved April 21, 2004, from http://www.businessweek.com/adsections/2003/pdf/0350security.pdf

Hruska, J. (1992). *Computer viruses and anti-virus warfare.* Great Britain: Ellis Horwood.

Hubbard, J.C., & Forcht, K.A. (1998). Computer viruses: how companies can protect their systems. *Industrial Management & Data Systems,* 98 (1), 12–16.

HyperDictionary. (2003). *Framework: dictionary entry and meaning.* Retrieved May 19, 2004, from http://www.hyperdictionary.com/dictionary/framework

Ibrahim M.S., Fakharu'l-razi A., & Aini M.S. (2003a). A review on disaster and crisis. *Disaster Prevention and Management, 12* (1), 24-32.

Ibrahim M.S., Fakharul-razi A., & Sa'ari M. (2003b). Technological disaster's criteria and models. *Disaster Prevention and Management, 12* (4), 305-311.

Infotech Research Group. (2003). *Building a comprehensive disaster recovery plan.* Retrieved April 10, 2004, from http://www.infotech.com/drp/full_sample.pdf

Jaring Internet Magazine. (2004). *MyDoom-F worm poised to attack Microsoft and record industry websites.* Retrieved April 19, 2004, from http://www.magazine.jaring.my/2004/february/index_stay.html?id=598&month=february&year=2004.

Jordan, E. (1999). IT contingency planning: management roles. *Information Management & Computer Security, 7* (5), 232-238.

Karakasidis, K. (1997). A project planning process for business continuity. *Information Management and Computer Security, 5* (2), 72-78.

Kelly, C. (1995). A framework for improving operational effectiveness and cost efficiency in emergency planning and response. *Disaster Prevention and Management, 4* (3), 25–31.

Kundu, S.C. (2004). Impact of computer disasters on information management: a study. *Industrial Management & Data Systems, 104* (2), 136-143.

Maiwald, E., & Sieglein, W. (2002). *Security planning & disaster recovery.* California: McGraw-Hill Osborne

MAMPU (2002a). *Rangka dasar keselamatan teknologi maklumat dan komunikasi kerajaan.* Retrieved April 5, 2004, from http://www.mampu.gov.my/ICT/MyMIS/AppendixA.PDF

MAMPU. (2002b). *The Malaysian Public Sector ICT Management Security Handbook.* Retrieved April 5, 2004, from http://www.mampu.gov.my/ICT/MyMIS/chapter3.PDF

Manecksha, F. (2004). *Warnings of more worm attacks.* Retrieved April 19, 2004, from http://www.niser.org.my/news/2004_05_10_01.html

Maslen, C. (1996). "Testing the plan is more important than the plan itself". *Information Management & Computer Security, 4* (3), 26-29.

McIvor, R. (2000). A practical framework for understanding the outsourcing process. *Supply Chain Management: An International Journal, 5* (1), 22-36.

Mills, A. (1995). Inadequate security encourages the thief. *Industrial Management & Data Systems, 95* (2), 3-5.

Muir, A., & Shenton, S. (2002). If the worst happens: the use and effectiveness of disaster plans in libraries and archives. *Library Management, 23* (3), 115-123.

MyCERT. (2004). *Situational report on major worms outbreaks up to year 2003 in Malaysia.* Retrieved April 5, 2004, from http://www.mycert.org.my/other_resources/NISER-MYC-PAP-7070-1.pdf

MyCERT, & NISER. (2004). *Incidents statistics.* Retrieved April 13, 2004, from http://www.mycert.org.my/

Nemzow, M. (1997). Business continuity planning. *International Network of Management, 7*, 127=136.

Neubauer, B.J., & Harris, J.D. (2002). Protection of computer systems from computer viruses: ethical and practical issues. *Journal of Consortium for Computing Sciences in Colleges, 18* (1), 270-279.

Paton, D. (1999). Disaster business continuity: promoting staff capability. *Disaster Prevention and Management, 8* (2), 127-133.

Polk, W.T., Wack, J.P., Bassham, L.E., & Carnahan, L.J. (1995). *Anti-virus tools and techniques for computer systems.* New Jersey: Noyes Data Corporation.

Raja, K.I., & Kakoli, B. (2000). Managing technology risk in the healthcare sector. *Disaster Prevention Management, 9* (4), 257-270.

Records Management. (2003). *What is a disaster?* Retrieved January 1, 2004, from http://www.umsystem.edu/records/dpa1.html

Reese, R.L.R. (2003). Incident handling an orderly response to unexpected events. *Proceedings of the SIGUCCS, USA,* 97-102.

Reuters. (2004). *Doomjuice worm aims at Microsoft.* Retrieved April 19, 2004, from http://www.wired.com/news/infostructure/0,1377,62229,00.html

Robbins-Gioia. (2003). *Preparing for the worst: a best-practices guide to disaster recovery.* Retrieved March 1, 2004, from http://www.gcn.com/Resource/disaster.pdf

Rohde, R., & Haskett, J. (1990). Disaster recovery planning for academic computing centers. *Communication of the ACM, 33* (6), 652-657.

Ruslan, R., Norazuwa, M., & Norazila, M. (2001). The implementation of disaster recovery planning (DRP) for information technology in Malaysia: a case of higher learning institutions. *The 2nd International Conference on Disaster Management, 2001,* Preparing and Planning for the Future, Surabaya, 1-10.

Sanderson, E., & Forcht, K.A. (1996). Information security in business environment. *Information Management and Computer Security, 4* (1), 32-37.

Savage, M. (2002). Business continuity planning. *Work Study, 51* (5), 254-261.

Schneiderman, B. (1998). *Designing the user interface: strategies for effective human computer interaction.* 3rd Edition, USA Addison Wesley Longman, Inc.

Sherif, J.S., & Gilliam, D.P. (2003). Deployment of anti-virus software: a case study. *Information Management & Computer Security, 11* (1), 5-10.

Shread, P. (2003). *Disaster recovery still just an IT responsibility.* Retrieved November 18, 2003, from http://www.enterprisestorageforum.com/industrynews/article.php/3072581

Sophos Plc. (2004). *Mystery surrounds tip-off to Microsoft about Sasser worm culprit, Sophos comments.* Retrieved May 18, 2004, from http://www.sophos.com/virusinfo/articles/sasserreward.html

Swann, J. (2004, February). Be prepared: disaster recovery strategies. *Community Banker,* pp. 40-44.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J., & Thomas, R. (2002). *Contingency planning guide for information technology systems: recommendations of the National Institute of Standards and Technology.* Retrieved May 19, 2004, from http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Sybase, Inc. (2003). *When disaster strike, recovery isn't enough.* Retrieved Mac 28, 2004, from http://www.sybase.com/content/1026317/5856_Disaster_Recovery_WP8.pdf

TechTarget. (2003). *Spiral model.* Retrieved April 24, 2004, from http://searchvb.techtarget.com/sDefinition/0,,sid8_gci755347,00.html

Tipton, H.F., & Krause, M. (2000). *Information security management.* United States of America: Auerbach Publications.

Toigo, JW. (1989). *Disaster recovery planning: managing risk and catastrophe in information systems.* New Jersey: Yourdon Press Computing Series.

Trend Mico, Inc. (2003). *Beyond layers and peripheral antivirus security.* Retrieved May, 29 from http://www.trendmicro.com/NR/rdonlyres/BD8EAA1F-477A-470A-9C19-4A1D347A9F4D/7870/WP01AVNP030703US.pdf

Universiti Utara Malaysia Computer Centre (2002a). *Dasar Keselamatan Rangkaian.* Retrieved April 4, 2004, from http://pkomputer.uum.edu.my/doc/DICT-04-2002.pdf

Universiti Utara Malaysia Computer Centre (2002b). *Objective and mission.* Retrieved April 4, 2004, from http://www.pkomputer.uum.edu.my/eng/index.php?page=pengenalan.php

Universiti Utara Malaysia Computer Centre (2003c). *10 virus terbanyak menyerang sistem komputer di UUM.* Retrieved April 15, 2004, from http://virus.uum.edu.my/utama.htm

Universiti Utara Malaysia Computer Centre. (2003d). *Gangguan Email, Serangan Virus...* Retrieved April 4, 2004, from http://pkomputer.uum.edu.my/index.php?page=bait_pengarah_sum.php

Weaver, J. (2003). *Disaster response and recovery.* Retrieved May 23, 2004, from http://www.hill.com/archive/pub/papers/2003/09/paper.pdf

Weckman, J., Colvin, T., Gaskins, R.J., & Mackulak, G.T. (1999). Application of simulation and the Boehm spiral model to 300-mm logistics system risk reduction. *Proceeding of the 31st Conference on Winter Simulation: Simulation - A Bridge to the Future, USA, 1,* 912-917.

Weichselgartner, J. (2001). Disaster mitigation: the concept of vulnerability revisited. *Disaster Prevention and Management, 10* (2), 85-94.

Wen, H. J. (1998). Internet computer virus protection policy. *Information Management & Compute Security, 6* (2), 66-71.

Whitman, M.E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, 46* (8), 91-95.

Williams, R., & Cummings, S. (1993). *Jargon: an informal dictionary of computer terms.* Barkely: Peachpit Press.

Wing, S.C. (2000). Success factors for IS disaster recovery planning in Hong Kong. *Information Management & Computer Security, 8* (2), 80-86.

Wood, C.C. (1996). A computer emergency response team policy. *Information Management & Computer Security, 4* (2), 4.

Zahri, Y., & Ahmad, N.M.Z. (2003). *Cyber threats: myths or reality?* Retrieved April 1, 2004, from http://www.niser.org.my/resources/cyber_threats.pdf