# DATA DISASTER RECOVERY MODEL FOR THE ASSOCIATION OF BUREAUX DE CHANGE OPERATORS OF NIGERIA, ABCON NIGERIA

ABUBAKAR MAGIRA TOM

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

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2015

This project is dedicated to my beloved family for their limitless support and inspiration.

# ACKNOWLEDGEMENT

Firstly, I would thank ALLAH (SWT) for giving the strength and guidance to successfully complete this research project. I take this opportunity to express my profound gratitude and deep regards to my guide PM. Dr. Norafida Binti Ithnin for her exemplary guidance, monitoring and constant encouragement through the course of this thesis. The blessing, help and guidance given by her time to time shall carry me a long way in the journey of life on which I am about to embark.

I am obliged to staffs of ABCON Nigeria for their valuable feedback and recommendations provided by them and grateful for their cooperation during the period of my project.

I thank my project examiner Dr. Maheyzah MD Siraj and DR. Yahaya Coulibaly for their support and guidance throughout my research.

Lastly, i thank my beloved parents, sisters, wife and friends for their constant support and encouragement without which this project would not be possible

# ABSTRACT

Disaster recovery planning is an active topic that has become a necessity for each and every organisation whether small, medium or large business. Disaster recovery elements of the contingency planning are taken lightly in most organisations. Disaster recovery Planning is the preparation for disaster whether artificial or natural causes. The domain includes several activities, methods and strategies in implementing and recovering data in the advent of disaster scenario. Thus, due to the threats faced by ABCON Nigeria namely virus, infected emails (spam), data loss or theft and human error, ABCON does not have an up-to-date disaster recovery model that will help in recovering their key business functions during and after disaster. Lack of employee security awareness training can make the organisation stagnant during disaster scenario. A data disaster recovery model is proposed to the organisation to mitigate and recover their important data to ensure business continuity and confidentiality of critical documents. The data disaster recovery model has six phases which are disaster preparedness, disaster risk assessment, disaster prevention, disaster response, immediate disaster recovery and documentation and lesson learnt concurrently. The proposed data disaster recovery model will be validated using questionnaires by experts in ABCON.

# ABSTRAK

Rancangan pemulihan bencana adalah satu topik yang aktif yang telah menjadi satu keperluan bagi setiap dan setiap organisasi sama ada perniagaan kecil, sederhana atau besar. Elemen pemulihan bencana perancangan luar jangka yang diambil ringan dalam kebanyakan organisasi. Perancangan pemulihan bencana adalah persediaan untuk bencana sama ada sebab-sebab semula jadi atau buatan . Domain ini termasuk beberapa aktiviti, kaedah dan strategi dalam melaksanakan dan memulihkan data dalam kemunculan senario bencana. Oleh itu , disebabkan ancaman yang dihadapi oleh ABCON Nigeria iaitu virus , e-mel yang dijangkiti (spam), kehilangan data atau kecurian dan kesilapan manusia, ABCON tidak mempunyai model up-to - tarikh pemulihan bencana yang akan membantu dalam memulihkan fungsi perniagaan utama mereka semasa dan selepas bencana. Kekurangan latihan kesedaran keselamatan pekerja boleh membuat organisasi bertakung dalam senario bencana. Pemulihan bencana model data adalah dicadangkan kepada organisasi untuk mengurangkan dan memulihkan data penting bagi memastikan kesinambungan perniagaan dan kerahsiaan dokumen kritikal. Pemulihan bencana model data mempunyai enam fasa yang persiapan menghadapi bencana, penilaian risiko bencana, pencegahan bencana , bantuan bencana alam, pemulihan bencana serta-merta dan dokumentasi dan pengajaran dipelajari serentak. Dicadangkan model pemulihan bencana data akan disahkan dengan menggunakan soal selidik oleh pakar-pakar dalam ABCON.

# TABLE OF CONTENTS

## LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| CP | Contingency Planning |
| DRP | Disaster Recovery Planning |
| CSIRTs | Computer Security Incident Response Teams |
| DR | Disaster Recovery |
| BCP | Business Continuity Planning |
| IRP | Incident Response Planning |
| IRT | Incident Response Team |
| NIST | National Institute Standard of Technology |
| PDCA | Plan Do Check Act |
| ACL’s | Access Control Lists |
| MAC | Mandatory Access Control |
| DAC | Discretionary Access Control |
| RBAC | Role Based Access Control |
| HS | Hot Site |
| WS | Warm Site |
| CS | Cold Site |
| CSP | Cloud Service Provider |
| CC | Cloud Computing |
| FI | Forensic Investigation |
| IS | Information Security |
| DRS | Disaster Recovery Site |
| SLA | Service Level Agreement |
| RPO | Recovery Point Objective |
| RTO | Recovery Time Objective |
| RAID | Redundancy Array Of Inexpensive Disk |
| HW | Hardware |

| | |
|---|---|
| SW | Software |
| ISO | International Organisation for Standard |
| HD | Hard Disk |
| CD’s | Compact Disks |
| DRA | Disaster Risk Assessment |
| BDC | Bureaux De Change |
| ABCON | Association Of Bureaux De Change Operators In Nigeria |
| CBN | Central Bank Of Nigeria |

## LIST OF APPENDIX

# CHAPTER 1

# INTRODUCTION

## 1.1 Overview

Disaster recovery planning is an active topic that has become a necessity for each and every organisation whether small, medium or large business. Disaster recovery elements of the contingency planning are taken lightly in most organisations. Disaster recovery Planning is the preparation for disaster whether artificial or natural cause (Whitman *et al.,* 2013). Whitman *et al.,* (2013) states that over 90% of experiencing disruption at data centre lasting ten days, thereby forcing organisations into bankruptcy. Again, over 40% of companies that experience disaster never reopen there business. Thus, nearly 30% of companies experiencing a disaster fail within two years. The downtime as a function exposes large organisations to an average loss of 1 million dollar per hour, most companies strive to keep schedule up to 98% and therefore, 174 hours of availability are typically lost annually. Still, Disaster recovery is something that is un-predictable and un-stoppable because it can be man-made or natural disaster which cannot be perceived or seen by human to comprehend. Thus, whenever disaster strikes, there are always possibilities of partial or total failure of organisations information thereby hinders the organisation from recovering on time for business continuity. Disaster recovery plan is ultimately planning for business continuity in the event of disaster (Webopedia, 2014). Disaster interrupts operation for over 90% of businesses nearly half of which disrupts business for a period of five years (Luckey, 2009).

Disaster recovery planning is a vital component deployed to efficiently assure that critical systems of organisations are readily available for business continuity when disaster strikes (Tipot and Krause, 2010). The main goal and objective of disaster recovery planning for most organisations are to reduce overall risks to a minimal level when disaster strikes. Many companies never update their disaster recovery plan and just keep it get all dusty, its rear for organisation to review disaster recovery plan and make sure it meets their security goals and objective (Bucki J, 2014).

Organisations must deal with disaster (Khan, 2012). Disaster response and prevention policies are required for the continuity of organisation functionality when disaster strikes. According to Snedaker S., (2013) business continuity as well as disaster recovery planning is ever more in need as well as its importance to the success of business of all classes and sizes, with growing dependence on information systems and electronic data. Practically, all business need to have a comprehensive and holistic business continuity plan and disaster recovery plan. In a survey commissioned by SunGard, availability and Harris Interactive, where both are IT executives, based on their findings, accessibility of information crucial to their critical business accomplishment IT and 78% business (Harris, Wheeler and Kacmar, 2009). Fewer than half of business executives say business continuity and DR are vital to organisation’s successful business compared with hefty population of information technology executives 74% IT and 49% business (Harris, Wheeler and Kacmar, 2009). Thus, having an up-to-date data disaster recovery plan for ABCON will help in the organisations business continuity with minimal impact after disaster scenario.

## 1.2 Problem Background

The Association of the Bureaux De Change Operators of Nigeria ABCON originated from the vision of some BDC operators with efforts to form a setting of holiness in the trade of foreign exchange. Moreover, Nigeria was facing awful economic decline due to the limitations placed on foreign exchange by the Nigerian government's policy called "Structural Adjustment Program" (SAP) prevalent in the '80s. Nigerian government attempts to rationalise the shortage of foreign exchange in circulation, they initiate measures to control access to foreign currencies through forbidden number of transactions in the official foreign exchange market as well as brought in thorough documentation. This formed an enormous demand for foreign exchange outside government approved sources (Abconng, 2014). These strict boundaries on performance at the parallel market gave boost to a growing issue of naira instability which by insinuation resulted to economic inflation. The Central Bank of Nigeria CBN, in an effort to freeze the hostile trend of naira instability and inflation, the CBN in 2006 brought in bureaux de change operator (BDC's) in the country into official market, with the aim of encouraging BDC's to purchase at official exchange rate as well as sell it to end-users within a permitted margin.

The Nigerian apex bank introduced cash sale of dollar to BDC Operators in Nigeria. Additionally, with the official empowerment of BDC's Operators in the Nigeria to observe to the selling and buying of foreign exchange, the juncture was set for officials in the financial sector to work efficiently and effectively (Abconng, 2014). ABCON is using normal mode of operation (traditional) by having all their systems and servers located in same location. According to Snedaker S., (2013), business continuity planning as well as disaster recovery planning has become vital to business of all classes and sizes. Yet, it increases reliance on information systems and electronic data, virtually all business need to have a comprehensive and holistic business continuity plan and disaster recovery plan. Nowadays, organisations have expensive equipment's that keep their business running and provide customers satisfaction with regard to confidentiality, availability and integrity. Most importantly, data should be readily available and provided to clients and organisations partners at all the time. However, any single failure can be costly to the organisation and its clients.

Disaster scenario can happen at any time either internal or external; therefore organisations must take preventive measures to protect the organisations assets and the required strategies for proper planning against disaster scenarios (Lufaj, 2012). Disaster recovery model for ABCON would help reduce causes of data loss from virus, infected email (spam), human error and data loss or theft and provide suitable activities and stages to mitigate and reduce the impact of the risks to ensure recovery of key business functions and business continuity within short period of time.

## 1.3 Problem Statement

The Association of Bureaux De Change Operators of Nigeria manages all independent bureaux de change operators in the Nigeria. There are thousands of bureaux de change operators that are managed by the company and all their transactions solely depend on ABCON. Currently, ABCON faces security threats of viruses, infected emails (spam), data loss or theft and human error. Thus, all these threats can be disastrous not only to ABCON but their customers as well. ABCON deals with a lot of customers and their critical information are stored in the organisation. Technology makes work faster and easier but it also comes with disadvantages that can be used to cause harm. Due to the weaknesses in technology, ABCON needs to have an up-to-date disaster recovery model that will help them in reducing threats that may cause data loss in the organisation. Protecting the confidentiality, integrity and availability of customer’s information is critical to ABCON.

ABCON adopts diverse techniques in mitigating threats, such as virus attacks, data loss, human error or spam (infected email). The critical issues that may arise from these attacks and may cause the organisation to run out of business as well affect their clients business. If an employee deletes critical files intentionally it will affect the reputation of ABCON as well as their customers.

So based on the above scenario, ABCON should have an up-to-date data disaster recovery model that will determine their business continuity in the advent of disaster events and the recovery of lost data after disaster.

## 1.4 Project Aim

The aim of this project is to propose a data disaster recovery model for ABCON Nigeria.

## 1.5 Project Objectives

The objectives  of this project are: -

i. To study existing disaster recovery models and select best practice model for ABCON.

ii. To propose a data disaster recovery model that will help in mitigating and reducing threats, that cause data loss, such as virus, data loss or theft, infected emails (spam) and human error.

iii. To evaluate and validate the proposed data disaster recovery model.

## 1.6 Scope

This project focuses on proposing a Data Disaster Recovery Model for ABCON Nigeria that will lessen the impact of virus attacks, data theft or loss, human error, and infected emails (spam). The proposed model will be validated by experts by giving out questionnaires to get their feedback and recommendations on the proposed data disaster recovery model.

## 1.7 Significance of the Project

This study will aid in providing a data disaster recovery model for ABCON Nigeria. A good practice disaster recovery model can help organisation to recover their critical data during and after disaster scenario. Due to the fact that cyber-crime is on the rise, this study will help the organisation in recovering from disaster.

## 1.8 Research Question

The research questions will help the author in channelling research in an efficient manner as well as provide guide lines via out the project. The research questions in this project include the following:-

i. What are the current threats to ABCON?
ii. What are the current methods in disaster recovery?
iii. What will be the impact caused by threats to ABCON?
iv. How will the proposed data disaster recovery model address the security issues faced by the organisation?

## 1.9 The Organisation of Report

This study comprise of six chapters, where each chapter describes unique information. Chapter one comprises of overview of the report, problem background, problem statement, aim and objectives of the project, scope, research questions, and organisation of the report

Chapter two highlights the review of the existing disaster recovery models, techniques, practices and activities to be carried out in the advent of disaster scenario. Chapter 3 consists of the research methodology and the flow in the project. Thus, the operational framework is also described in this chapter.

Chapter four is the analysis and design phase which consists of the proposed data disaster recovery model, guidelines, techniques and activities to be conducted in each phase on how to recover and contain incident in the advent of disaster scenario.

Chapter five comprises the results and the validation of the proposed data disaster recovery model, the feedback from the review and criticism from experts are as well discussed in this chapter.

Chapter six is the final chapter in this study. The achievements, reviews and limitations and future enhancement of this study are described in this chapter.

# REFERENCES

Anderson, R. 2009. Why information security is hard-an economic perspective. Computer Security Applications Conference, 2009. ACSAC 2009. Proceedings 17th Annual, IEEE.

Asghari, S. A., Pedram, H., Taheri, H., & Khademi, M. 2010. A New Background Debug Mode Based Technique for Fault Injection in Embedded Systems. International Review on Modelling & Simulations, 3(3).

BackUpSolutions. 2014. Back Up Solutions. [Online]Available: http://www.myhomeoffice.co.uk/backup.html. Last accessed 15th May 2014.

Bailey, M., et al. 2009. A survey of botnet technology and defenses. Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology, IEEE.

Bairavasundaram, L. N., G. R. Goodson, et al. 2007. An analysis of latent sector errors in disk drives. ACM SIGMETRICS Performance Evaluation Review, ACM.

Bandyopadhyay, K., Mykytyn, P. P., & Mykytyn, K. 2009. A framework for integrated risk management in information technology. Management Decision,37(5), 437-445.

Bartlett Learning.Reid, A. and J. Lorenz 2008. Working at a Small-to-Medium Business or ISP, CCNA Discovery Learning Guide, Pearson Education.

Bergstra, J. and M. Burgess. 2011. Handbook of Network and System Administration, Elsevier Science.

Budman, G. 2009. Causes of data loss and some statistics. [Online]Available: https://www.backblaze.com/blog/causes-of-data-loss-and-some-statistics/. Last accessed 13th Oct 2014.

Calder ,A and Watkins, S. 2012. IT Governance: An International Guide to Data Security and ISO27001/ISO27002. 5th ed. United States: Kogan Page Publishers. p9-12.

Cambridge. 2014. disaster. [Online]Available: http://dictionary.cambridge.org/dictionary/british/disaster?q=disaster. Last accessed 15th May 2014.

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

Chien, E. and Ször , P. 2002. "Blended attacks exploits, vulnerabilities and buffer-overflow techniques in computer viruses." Virus 1.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. 2012. Computer Security Incident Handling Guide. NIST Special Publication, 800, 61.Chicago reference

Cintech. 2014. What is a Firewall?. [Online]Available: http://www.cintech.co.uk/ITSST/coursecontent/09/9_04a.htm. Last accessed 15th May

Cisco. 2014. configuring failover. [Online]Available: http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm32/configuration/guide/fwsm_cfg/fail_f.html#wp1041883. Last accessed 13th Oct 2014.

Collins, L. R. 2009. Disaster Management and Preparedness.

Cooke, E., F. Jahanian, et al. 2009. The zombie roundup: Understanding, detecting, and disrupting botnets. Proceedings of the USENIX SRUTI Workshop.

Cpni. 2014. Business continuity planning. [Online]Available: http://www.cpni.gov.uk/Security-Planning/Business-continuity-plan/. Last accessed 22nd Apr 2014.

Disasterrecoveryplantemplate. 2013. Disaster Recovery Plan. [Online]Available: http://www.disasterrecoveryplantemplate.org/. Last accessed 1st May 2014.

Erbschloe, M. 2003. Guide to Disaster Recovery, Course Technology.

Farahmand, F., et al. 2003. Managing vulnerabilities of information systems to security incidents. Proceedings of the 5th international conference on Electronic commerce, ACM

Fry, C. and Nystrom , M. 2009. Security monitoring, " O'Reilly Media, Inc.".

Geoffrey H. Wold. 2014. Disaster Recovery Planning Process. [Online]Available: http://www.drj.com/new2dr/w2_002.htm. Last accessed 8th May 2014.

Gilbert, S. W. 2010. "Disaster resilience: A guide to the literature." US Department of Commerce, National Institute of Standards and Technology (NIST), Special Publication 1117.

Google. 2014. Nigerian. Available: https://www.google.com.my/?gws_rd=cr,ssl&ei=8V0WVIWoA8S8ugTS84LABw. Last accessed 15th Sep 2014.

Gregory, P.H., & Rothstein, P.J. 2011. IT Disaster Recovery Planning For Dummies: Wiley.

Harris, K. J., Wheeler, A. R., & Kacmar, K. M. 2009. Leader–member exchange and empowerment: Direct and interactive effects on job satisfaction, turnover intentions, and performance. The Leadership Quarterly, 20(3), 371-382.

Heng, G.M. 2009. A Manager's Guide to Implement Your IT Disaster Recovery Plan: GMH Pte Limited.

Herley, C. 2012. Why do Nigerian scammers say they are from Nigeria? WEIS.

Ifrc. 2014. Contingency planning. Available: http://www.ifrc.org/en/what-we-do/disaster-management/preparing-for-disaster/disaster-preparedness-tools/contingency-planning-and-disaster-response-planning/. Last accessed 22nd Apr 2014.

ISO. 2012. ISO 22301:2012 - Business Continuity Management System. [Online]Available: http://www.go4iso.com/iso-standards-their-enefits/iso-2-2012-business-continuity-management-system/. Last accessed 27th Apr 2014.

ISO. 2014. Standards What is a standard?. [Online]Available: http://www.iso.org/iso/home/standards.htm. Last accessed 5th May 2014.

James, K. 2011. The organizational science of disaster/terrorism prevention and response: Theory-building toward the future of the field. Journal of Organizational Behavior, 32(7), 1013-1032.

John R, P. D. C. and P. D. C. C. James F. R. 2011. Business Continuity and Disaster Recovery for InfoSec Managers, Elsevier Science.

Johnson, W. R. and M. Sanchez 2012. Virus/worm throttle threshold settings, Google Patents.

Kadav, A., Renzelmann, M. J. et al. 2009. Tolerating hardware device failures in software. Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles, ACM.

Kahn, M. B. (2012). Disaster Response and Planning for Libraries, American Library Association.

Kahn, M. B. 2012. Disaster response and planning for libraries. American Library Association.

kaspersky. 2013. kaspersky security bulletin. Available: http://report.kaspersky.com/. Last accessed 27th Apr 2014.

Kelley, O. 2009. How to Perform a Disaster Recovery Business Impact Analysis. Available: http://www.csoonline.com/article/2124593/emergency-preparedness/how-to-perform-a-disaster-recovery-business-impact-analysis.html. Last accessed 22nd Apr 2014.

King, R. 2012. Virus Aimed at Iran Infected Chevron Network. [Online]Available: http://online.wsj.com/news/articles/SB10001424127887324894104578107223667421796. Last accessed 27th Apr 2014.

Law, A. B. A. S. o. A. 2008. Data Security Handbook, American Bar Association

Li, M.-L., P. Ramachandran, et al. 2008. Understanding the propagation of hard errors to software and implications for resilient system design. ACM SIGARCH Computer Architecture News, ACM.

Lin, P. P. 2006. "System security threats and controls." CPA JOURNAL 76(7): 58.

Margaret, R. 2005. business impact analysis (BIA). [Online]Available: http://searchstorage.techtarget.com/definition/business-impact-analysis. Last accessed 22nd Apr 2014.

Mark, G. 2013. South Korea network attack 'a computer virus'. [Online]Available: http://www.bbc.com/news/world-asia-21855051. Last accessed 27th Apr 2014.

Meriam-webster. 2014. Security. [Online]Available: http://www.merriam-webster.com/dictionary/security. Last accessed 20th Sep 2014.

Microsoft. 2014. Common Types of Network Attacks. [Online]Available: http://technet.microsoft.com/en-us/library/cc959354.aspx. Last accessed 13th Oct 2014.

Ministry of Communication Technology. 2014. The 2014 Nigerian Cyber Threat Barometer Report. [Online]Available: wolfpackrisk.com/2014_Nigerian_Cyber_Threat_Barometer_(High_Res. Last accessed 15th Sep 2014.

Nicole, D. 2011. How Small Businesses Can Protect and Secure Customer Information. [Online]Available: http://www.sba.gov/blogs/how-small-businesses-can-protect-and-secure-customer-information. Last accessed 10th Oct 2014.

NIST. 2014. Disaster Resilience Framework and Guidance. [Online]Available: http://www.nist.gov/el/building_materials/resilience/framework.cfm. Last accessed 27th Apr 2014.

NIST. 2014. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. vol 1 (1), p5-10.

Nolting, D. 2013. RPO, RTO, PTO and RaaS: Disaster recovery explained. [Online]Available: http://www.bluelock.com/blog/rpo-rto-pto-and-raas-disaster-recovery-explained/. Last accessed 13th Oct 2014.

NPDN. 2014. Malicious Software: Viruses, Worms, and Trojan Horses. [Online]Available: http://www.npdn.org/infosec_sw_malware. Last accessed 27th Apr 2014.

Npdn. 2014. Malicious Software: Viruses, Worms, and Trojan Horses. [Online]Available: http://www.npdn.org/infosec_sw_malware. Last accessed 27th Apr 2014.

Owasp. 2006. File:OWASP 10 Most Common Backdoors. [Online]Available: https://www.owasp.org/index.php/File:OWASP_10_Most_Common_Backdoors.pdf. Last accessed 13th Oct 2014.

Owasp. 2013. The Ten Most Critical Web Application Security Risk. [Online]Available: https://www.owasp.org/index.php/Top_10_2013-Top_10. Last accessed 13th Oct 2014.

Owasp. 2013. Repudiation Attack. [Online]Available: https://www.owasp.org/index.php/Repudiation_Attack. Last accessed 13th Oct 2014.

Pau. 2014. Department of Information Processing: Hardware Problems. [Online]Available: http://www.pau.edu.tr/bidb/en/sayfa/hardware-problems. Last accessed 13th Oct 2014.

Rachael, K. 2012. Virus Aimed at Iran Infected Chevron Network. [Online]Available: http://online.wsj.com/news/articles/SB1000142412788732489410457810723667421796. Last accessed 27th Apr 2014.

Ramachandran, J. (2002). Designing Security Architecture Solutions, Wiley.

Ramesh, P.(2002). "Business Continuity Planning." Technology Review: 4.

Reid, A. and Lorenz, J. 2008. Working at a Small-to-Medium Business or ISP, CCNA Discovery Learning Guide, Pearson Education.

Rittinghouse J. P. D. C. and P. D. C. C. James F. R. 2011. Business Continuity and Disaster Recovery for InfoSec Managers, Elsevier Science.

Rothstein, P.J. 2007. Disaster Recovery Testing: Exercising Your Contingency Plan (2007 Edition): Rothstein Associates Incorporated.

Savage, M. 2002. "Business continuity planning." Work study 51(5): 254-261.

Schroeder, B. and G. A. Gibson. 2007. Understanding failures in petascale computers. Journal of Physics: Conference Series, IOP Publishing.

Shea, B. 2002. Have You Locked the Castle Gate?: Home and Small Business Computer Security, Addison Wesley Professional.

Silva, S. S., et al. 2013. "Botnets: A survey." Computer Networks 57(2): 378-403.

Snedaker, S. 2013. Business Continuity and Disaster Recovery Planning for IT Professionals, Elsevier Science.

Solomon, M. G. 2013. Security Strategies in Windows Platforms and Applications, Jones & Stephen, H., 2014. Remove Malware. [Online]Available: http://www.home-computer-support.org/remove-malware.html . Last accessed 15th May 2014.

Subashini, S., & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-1

Taylor & Francis. BS, T. 2014. Disaster Recovery and Business Continuity: A quick guide for small organisations and busy executives, IT Governance Publishing.

Techtarget. 2014. contingency plan. [Online]Available: http://whatis.techtarget.com/definition/contingency-plan. Last accessed 22nd Apr 2014.

Ten, C.-W., G. Manimaran, et al. 2010. "Cybersecurity for critical infrastructures: attack and defense modeling." Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on 40(4): 853-865.

Unp. 2012. Types of Attacks. [Online]Available: http://www.unp.me/f140/types-of-attacks-63305/. Last accessed 13th Oct 2014.

Vangie, B. 2014. Data. [Online]Available: data base simply refers to facts or figures as well as information that is stored and accessed by a computer system. Last accessed 25th Sep 2014.

Vellani, K. 2006. Strategic Security Management: A Risk Assessment Guide for Decision Makers, Elsevier Science.

Wells, A. J., et al. 2006. Disaster Recovery: Principles and Practices, Pearson Prentice Hall.

Wells, A. J., et al. 2006. Disaster Recovery: Principles and Practices, Pearson Prentice Hall.

Wen, H. J. 1998. "Internet computer virus protection policy." Information management & computer security 6(2): 66-71.

White, G. B., et al. 1995. Computer System and Network Security, Taylor & Francis.

Whitman, M. and Mattord H. 2011. Roadmap to Information Security: For IT and Infosec Managers, Cengage Learning.

Whitman, M. and Mattord, H. 2013. Management of Information Security, Cengage Learning.

Woodie, A. 2010. Human Error the Number One Cause of Data Loss, Survey Says. [Online]Available: http://www.itjungle.com/tfh/tfh072610-story10.html. Last accessed 10th Oct 2014.