CRITICAL INFORMATION ASSETS DISASTER MANAGEMENT AUDIT MODEL FOR UTM STUDENT INFORMATION SYSTEM

ABUBAKAR AMINU MU'AZU

A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Master of Science (Information Technology- Management)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MARCH 2010

ABSTRACT

In any modern universities like UTM, e-learning is an important technology that can improve the quality of teaching and learning. Information is constantly processed and combined to form new information assets that are critical to any business processes. The critical information assets perceived by UTM e-learning as the owner or stakeholders (such as Centre for Teaching & Learning (CTL), Centre for Information and communication Technology (CICT), students and lecturers) will suffer an adverse impact if the information assets are lost, interrupted or destroyed. Therefore, it becomes necessary for the owners of UTM e-learning to identify their critical information assets. This research is conducted on UTM e-learning system in identifying the critical information assets and type in which are being stored or held as well as identifying the potential threats (disasters) that might affect the information assets. The researcher adopted the use of Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, OCTAVE Allegro in identifying the critical asset and some models of information management. The research identifies the real information needs in UTM e-learning system by identifying who needs the information by putting together a good plan and auditing it regularly that can go a long way towards preventing a disaster. Eventually, a disaster audit model for the system was proposed that reflects the concept of critical information asset disaster control.

ABSTRAK

Dalam setiap universiti moden seperti UTM, e-learning adalah satu teknologi penting yang boleh meningkatkan lagi kualiti mengajar dan belajarMaklumat sentiasa diproses dan digabungkan untuk membentuk maklumat baru yang sangat penting kepada sebarang proses perniagaan. Aset maklumat kritikal yang dipercayai oleh e-learning UTM sebagai pemilik atau stakeholder (seperti Centre for Teaching & Learning (CTL), Centre for Information and communication Technology (CICT), mahasiswa dan pensyarah) akan merasai kesan yang merugikan jika aset maklumat hilang, terputus atau musal. Disebabkan perkara itu, adalah penting bagi pemilik e-learning UTM untuk mengenalpasti aset maklumat kritikal mereka Kajian ini dilakukan pada sistem e-learning UTM bagi mengenalpasti aset maklumat kritikal yang sedang disimpan atau dipegang serta mengenalpasti potensi ancaman (bencana) yang mungkin menjejaskan aset maklumat. Penyelidik menggunakan methodologi Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), OCTAVE Allegro dalam mengenalpasti kritikal aset dan beberapa model pengurusan maklumat. Bencana, samada semulajadi dan buatan manusia, boleh berlaku pada bila-bila masa atau di mana saja. Penyelidikan mengenalpasti keperluan maklumat sebenar di sistem e-learning UTM dengan mengenalpasti siapa yang memerlukan maklumat dengan menyusun perancangan yang baik dan diaudit secara teratur yang boleh pergi jauh ke arah mencegah bencana. Akhirnya, satu audit bencana model untuk sistem itu adalah dicadangkan yang mencerminkan konsep maklumat kritikal itu bencana aset kawalan.

TABLE OF CONTENTS

2. LITERATURE REVIEW

3. RESEARCH METHODOLOGY

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

eLearning system, with the identification of the critical information assets. Furthermore, it will also highlight the potential disasters that might cause temporary or extended loss to one or more of critical information assets. Priority attention would be paid to identifying the critical information assets owner. This is done by for ensuring that information is classified and authorized by the information owner and also to establish and maintain a register/inventory to record the security classification of each critical information asset. This will be achieved by examining all the critical information assets and identifying those which are essential to UTM student eLearning system in the event of a disaster.

1.2 Problem Background

University Computer-based Information Assets are any information relating to the business or interests of the University. Examples of these assets include planning documents, reports on the activities of the University, letters, memos, research papers, course material, and results from experiments. The loss of these assets would represent a loss to the University and may in some circumstance damage the University in some way (including damaging its reputation). The prospects of e-learning are immense. It continues to grow at a tremendous rate both in education and training.

Electronic exchange of information takes place within individual organisations as well as between them, typically reducing communication delays. For example, separate business units within a company use email to transfer documents almost instantly, whereas in the past they had to rely on a comparatively slow internal mail system. Highly efficient intra-organisational workflows are now possible through electronic communication.

However, these new forms of communication and commerce also present new dangers since they make an organisation's information assets subject to new threats. Access to vital assets may no longer be restricted to those who have a key for the lock of the door that protects a building. Electronic communication may make the whole world your market place; but there is a danger that it will also make the whole world your premises.

The disaster audit concept will start by identifying the critical information asset in the university computer-based information assets of the student information service; eLearning system. It is quite possible that the systems that receive, host, manipulate and transmit the organisation's information assets could be tampered. However, it is seldom to conduct a risk management which could identify the potential disasters that may cause temporary or extended loss to one or more of the critical information assets as well as developing and implementing cost-effective countermeasures to cope with these disasters.

1.3 Problem Statements:

As describe in the problem background section, the current issue need to be addressed in this project are as below:

- How to identify the critical information assets for UTM e-learning system?
- How are the critical information assets stored and retrieved?
- How the eLearning information assets are held?

1.4 Objectives of the Project

- To identify the critical information asset for UTM
- To identify the forms of which the Information Asset (records) are held.
- Identifying potential disasters that may cause temporary or extended loss to one or more of UTM students' eLearning systems.
- To develop and proposed a critical information asset disaster management audit model

.

1.5 Scope of the Project

The scope which identifies the boundaries of this project is:

- To study the Computer-Based Information system that support core business in UTM administrative services that is student Information System (E-learning)
- The study will only focus on the key and high level characteristics identified by means of the research methodology and approach followed.

1.6 Importance of the Project

This project is important for Universiti Teknology Malaysia (UTM) e-learning system in terms of:

- Controlling, protecting, delivering, and enhancing the value of data and information assets within the department.
- Recognising the dependence of most business upon Information and Communication Technology (ICT) infrastructure and the quantity, quality and availability on the information.
- Minimising the likelihood and impact (risk) of interruptions
- Ensuring the e-learning stakeholders know that every action they perform against the database can be audited.

1.7 Chapter Summary

The critical information asset (CIA) is basically the circulatory and nervous system of the organization. Instead of focusing on technology as a cost or expense, organizations can really begin to change this focus by understanding and utilizing the value of their data information asset. There is a huge opportunity to collect, store, transform and present information and knowledge to users to increase the effectiveness of reporting and decision making across the organization and at all levels.

Research regarding critical information asset will be explored to determine the systematic steps that can be applied in the event of disaster recovery using disaster audit approach in UTM e-learning system. Appropriate questions will be created based on the core processes to identify the critical information asset in the eLearning system. The management audit model will be developed to help in managing information after conducting CIA disaster audit, based on the information provided by the UTM, students’ e-learning stakeholders, which e-learning service administrators, instructors and students.

REFERENCE

ABREMA (08:2009) Activity Based Risk Evaluation Model of Auditing, available at http://www.abrema.net/abrema/audit_approach_g.html *(Retrieved on 26/08/09)*

Adnan e tl (2006). A journal of The Role of GIS and Public Awareness for Disaster Management.

April W., Charlyne W. and Timothy W. (2007) Disaster Recovery Principles and Practice. Pearson Prentice Hall.

Avinash Kadam, (2001) Network security Magazine; available at http://www.networkmagazineindia.com/200212/security2.shtml *(Retrieved on 15/08/09)*

Berdie, D. 1973. "Questionnaire length and response rate." Journal of Applied Psychology 58:278-280.

Buchanan, S. and Gibb, F. (1998). The information audit: an integrated strategic approach. International Journal of Information Management,18(1), pp. 29–47.

Business Continuity Planning, Recovery Strategy. See also Business Continuity Planning Guidelines, available at http://www.dir.state.tx.us/security/policies *(Retrieved on 28/08/09)*

Charles Oppenheim (2001) journal “The attributes of information as an asset” MCB unicesity press

Chun Wei Choo (1998) Information Management for the Intelligent Organization: *The Art of Scanning the Environment*, 2nd Edition 272 pages, hardbound

CISA (Certified Information Systems Auditor) 2006. CISA Review Manual

Continu Data Service (28:08:09) Keeping your business in play available at; www.continu.net/disaster-recovery-planning *(Retrieved on 06/09/09)*

Cost of Information Assurance (2002). The National Center for Manufacturing Sciences, University of Michigan Tauber Manufacturing Institute www.tmi.umich.edu *(Retrieved on 10/08/09)*

DIR State of Texas (2003) Practices for Protecting Information Resources Assets, Leadership for Texas Government Technology

Drucker, P (1993), *Post-capitalist Society*, Butterworth-Heinemann, Oxford

Gartner Newsroom (2006) , "Says Start Managing Information, Not Just Technology", Egham, UK, October 25, 2006.

Goode, W., and P. Hatt. 1962. Methods in Social Research New York: McGraw-Hill.

Guidelines for Information Security Policy, 2001 available at: http://www.kantei.go.jp/foreign/it/security/2001/g3.html *(Retrieved on 26/08/09)*

Harasim, L., Hiltz, S. R., Teles, L. and Turoff, M. (1995) Learning Networks: A Field Guide to Teaching and Learning Online, The MIT Press, Cambridge.

Henczel S. (2000), the information audit as a first step towards effective knowledge management: an opportunity for the special librarian, INSPEL 34(2000)3/4, pp. 210-226.

Henczel, S. (2001), The Information Audit: A Practical Guide, KG Saur, Munich.

Hoffer, Jim. "Backing Up Business - Industry Trend or Event." Health Management Technology, Jan 2001

Jamaica archive (07:2009) Protecting Our Information Assets, in observance of Records & Information Management Month, available at http://www.jard.gov.jm/records/content/view/36/2 *(Retrieved on 12/08/09)*

Jintae L& Tung B. (2000). A Template-based Methodology for Disaster Management Information Systems. Proceedings of the 33rd Hawaii International Conference on System Sciences.

Johnson, John D (1999). "Conducting Risk Analysis to Evaluate Enterprise Security." *Security Portal.*

Laudon K, & Laudon J. (2006): "Management Information Systems – *Managing the digital firm* 9th Edition ." Pearson – Prentice Hall.

Learning space, http://openlearn.open.ac.uk/mod/resource/view.php? *(Retrieved on 26/08/09)*

Lucy, R.F. 1999. "IS Auditing: The State of the Profession Going into the 21st Century". Information Systems Audit & Control Journal, 4:44-50.

Marlia Puteh, (2008) "e-Learning Implementation in Malaysian Universities: The Universiti Teknologi Malaysia Experience". Proceedings of the 3rd International Conferences on e-Learning, University of Cape Town South Africa, 26-27 June 2008.

Mouton, J. 2005. How to Succeed in Your Master's & Doctoral Studies, A South African guide and Resource Book. Pretoria: Van Schaik Publishers.

Nicole Wagner, Khaled Hassanein & Milena Head (2006) E-Learning in Higher Education: A Stakeholders' Analysis.

OECD SIGMA (1998): Effects of European Union Accession, Part 1: Budgeting and Financial Control, OECD SIGMA Paper No. 19, Appendix 3: List of Useful Terms.

Olivier, M.S. 2004. Information Technology Research, A Practical Guide for Computer Science and Informatics. 2nd edition. Pretoria: Van Schaik Publishers.

Page, C. & Meyers, D. 2003. Applied Research Design for Business and Management. Sydney: The McCraw-Hill Companies, Inc.

Patel R. & Davidson B. (1994) Forskningsmetodikens Grunder att Planera, Genomföra och Rapportera en Undersökning, Student literature.

Paul F. Kirvan (2009): Minimizing business risk with disaster recovery audits. Available at: http://searchdisasterrecovery.techtarget.com/generic *(Retrieved on 12/11/09)*

Richard et' l (2007) Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process Technical Report CMU/SEI-2007-TR-012 ESC-TR-2007-012

Sheila & Peter (2002) The internal information audit: conducting the audit and implementing the results.

Steven Buchanan, Forbes Gibb (2007) International Journal of Information Management, 159–172

Whitman & Mattord (2008) Management of Information Security, second edition, Kennesaw State University Course Technology Cengage Learning.

.