THREATS TO ELECTRONIC RECORDS SECURITY IN THE MALAYSIAN GOVERNMENT ORGANIZATIONS

RESEARCH MANAGEMENT INSTITUTE (RMI)
UNIVERSITI TEKNOLOGI MARA
40450, SHAH ALAM, SELANGOR

BY:
AHMAD AZMAN BIN MOHAMAD RAMLI
NOR ZAINA ZAHARAH BINTI MOHAMAD ARIFF
DR. WAN AB KADIR BIN WAN DOLLAH

FEBRUARI 2012

Contents

PENGHARGAAN

Setinggi-tinggi penghargaan dan ribuan terima kasih diucapkan kepada semua pihak yang terlibat secara langsung dan tidak langsung bagi membolehkan penyelidikan ini disiapkan dengan sempurna.

Di antaranya:

Prof. Madya Dr. Haji Laili Haji Hashim
(Dekan Fakulti Pengurusan Maklumat, Universiti Teknologi MARA)

Profesor Dr. Abu Bakar Abdul Majeed
(Penolong Naib Canselor (Penyelidikan), Institut Pengurusan Penyelidikan)

Prof. Madya Dr. Mohd Sharif Mohd Saad
(Timbalan Dekan Penyelidikan dan Jaringan Industri, Fakulti Pengurusan Maklumat)

Encik Osman Abd. Aziz
(Pengarah Bahagian Pematuhan ICT,MAMPU, Jabatan Perdana Menteri)

Puan Sophia Hashim
(Bahagian Pematuhan ICT,MAMPU, Jabatan Perdana Menteri)

EXECUTIVE SUMMARY

Malaysian government organizations which are engaging in conducting public business have many reasons to protect their records security from any threats, regardless the format of the records. Some of the reasons are as follows: first, the records are a national heritage containing important information pertaining to the country's administration and history. Second, the government organizations conduct business on the behalf of the public, and their records contain information that documents the rights and interests of the public and government. Unfortunately, records in an electronic format are more vulnerable to any threats and less secure than records in a paper format. For example, deleting electronic records accidentally without realizing it and entering data wrongly are common mistakes among staff in any organizations. Furthermore, intentional security threats in the form of hacking, malicious attacks on network, and frauds involving electronic records are all common occurrences in any organizations. Hence, in line with this situation, this paper attempts to study and understand the various types of threats to electronic records security in the Malaysian government organizations. This paper also aims to recommend several possible techniques to protect the records security. This study is based on two techniques to collect data. The techniques are content analysis for studying the content of a website and a review of documentation, such as books, article journals, seminar papers, circulars, newspapers, magazines and reports from non-government and government organizations that are relevant to the scope of the study. The findings show that there are several threats to electronic records at Malaysian government organizations, such as human errors and omission, electric power irregularities, espionage or trespass, employee crime, theft and fraud, malicious codes, denial of services (dos) attacks, force of nature, technical hardware failure, technical software failure and technological obsolescence. Hence, in order to protect the electronic records, there are several techniques that have been identified, namely: virus protection software, controlling access, audit trails, backup and recovery mechanism, establish network security systems, store vital electronic records offsite, establishing a disaster preparedness plan and a security awareness program for staff.

Keywords: *Records, Electronic Records, Records Security, Records Threats, Records Protection Techniques.*

4.2. INTRODUCTION

4.2.1. INTRODUCTION

Malaysian government organizations have many reasons to protect their records security from any threats, regardless of the format of the records. Some of the reasons are as follows: First, the records are national heritage containing important information pertaining to the country's administration and history. Second, the government organizations conduct business on the behalf of the public, and their records contain information that documents the rights and interests of the public and government.

Unfortunately, records security in an electronic format is more vulnerable to any threats and less secure than records in a paper format. For example, deleting electronic records accidentally without realizing it and entering data wrongly are common mistakes among staff in any organizations. Furthermore, intentional security threats in the form of hacking, malicious attacks on network, and frauds involving electronic records are also common occurrences in any organizations. Hence, in line with this situation, this study attempts to highlight the various types of threats to electronic records security in the Malaysian government organizations. In addition, it also aims to recommend possible techniques to protect the records.

4.2.2. STATEMENT OF PROBLEM

Having the awareness of the vulnerability of electronic records to any threats, Malaysian government has conducted several strategies and programs to protect its electronic records. For example, it has established Government Computer Emergency Respond Team (GCERT) on January 2001. This organization is one of the sections under Information and Communication Technology (ICT) Security Division at MAMPU. Its main objectives are to ensure the continuity of government organization businesses and to combat the threats to electronic records in Malaysian government organizations. Furthermore, Department of Public Service has produced and circulated several handbooks and circulars to government organizations regarding the policy and methods to protect electronic records. For example, on October 1, 2000, it has circulated General Circular regarding a policy framework on ICT security in Malaysian government organization. On January 15, 2001, it produced Malaysian Public Sector Management of Information and Communications Technology Security Handbook. On November 7, 2005, it has circulated guidelines pertaining to the evaluation of information security in public sectors.