A DIGITAL FORENSIC READINESS COMPONENTS FOR OPERATIONAL UNIT

ABDULALEM ALI MOHAMMED SALEH

A project 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

JUNE 2013

This project is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisor **Dr. Norafida Ithnin** for her constant support during my study at UTM. She inspired me greatly to work in this project. Her willingness to motivate me contributed tremendously to our project. I have learned a lot from her and I am fortunate to have her as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as employees in CICT help me to validate the project and gave me some information which I need during validation process.

Last but not the least, I would like to thank my family especially my parents and my wife, for encouraging me to complete my postgraduate studying of master degree and supporting me spiritually throughout my life.

ABSTRACT

The growing threats of fraud and security incidents present numerous of challenges to law enforcement and organizations widespread the world. This has given rise to the need for organizations to make effective incident management strategies, that will improve the company's ability to react to security incidents. Most of organizations underestimate the demand for digital evidence. A forensic investigation of digital evidence is commonly employed as a post-event response to a serious information security incident. In fact, there are many circumstances where an organization may benefit from an ability to gather and preserve digital evidence before an incident occurs. Digital forensic readiness enables an organization to maximize its potential to use digital evidence whilst minimizing the costs of an investigation. In order to ensure organizations ready for incidents must implement the digital forensics readiness in workplace environment. This research aims to identify from existing studies, the concept of digital forensic readiness and how they apply to operational unit. This study focus on previous frameworks and analysis, compare among them to combining and integrating their major components to propose appropriate components of digital forensic readiness for operational unit. These components will help managers and staff to comply with digital forensic discipline in their organization.

ABSTRAK

Ancaman penipuan dan insiden keselematan yang semakin meningkat menyebabkan pelbagai cabaran untuk penguatkuasaan undang-undang dan organisasi meluas dunia. Ini telah menimbulkan keperluan bagi organisasi untuk melakukan strategi pengurusan insiden yang berkesan, iaitu yang akan meningkatakan keupayaan organisasi itu untuk bertindak terhadap insiden keselamatan. Kebanyakan organisasi memandang mudah permintaan bukti digital. Penyiasat Forensik bukti digital kebiasaanya bertindak selepas insiden keselamatan makulumat berlaku. Malah, terdapat banyak keadaan dimana organisasi boleh mendapat faedah dari keupayaan mengumpulkan dan memelihara bukti digital sebelum berlakunya insiden. Kesedian Forensik Digital membolehkan sesuatu organisasi memaksimumkan potensinya menggunakan bukti digital dalam pada masa yang sama meminimumkan kos penyiasatan. Dalam usaha memastikan organisasi bersedia menghadapi insiden, ia mesti melaksanakan kesediaan forensic digital dalam suasana tempat kerja. Kajian ini bermatlamatkan untuk mengenalpasti daripada kajian sedia ada, konsep kesediaan forensic digital dan bagaimana mereka menjalankan di unit operasi. Kajian ini memfokuskan pada rangka kerja dan analisis sebelum-sebelum ini, membanding dan mengintegrasikan komponen utama mereka untuk mencadangkankomponen kesediaan forensic digital yang sesuai bagi unit operasi. Komponen ini akan membantu pengurus dan pekerja mematuhi forensic digital disiplin di dalam organisasi mereka.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGUERS

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Growing threats of fraud and security incidents lead to numerous challenges for law enforcement and organizations all over the world. This has led to the need for organizations to build effective strategies to manage incidents, that will improve the company's ability to react to security incidents.

Most organizations ignore the requirements of digital forensics. For example, when there is a need to verify the authenticity of evidence of fraudulent transactions, there is no enough evidence for trustworthy linking attacker accident or attack. Therefore this it is necessary for organizations to prepare themselves for the digital forensic investigations and ensure that they are preparing a full regulatory environment for investigation.

In order to ensure organizations readiness for incidents, they should implement the digital forensics readiness in the workplace environment. Digital forensic readiness (DF readiness) is the ability of an organization to maximize its possible to use the electronic evidence when necessary. DF readiness assists organizations to improve their security approach, minimize the effect of security incidents. Indeed , there are many cases where an organization could benefit from having the ability to collect and preserve digital evidence before an incident occurs. DF readiness helps an organization to maximize its ability to use digital evidence

while reducing the cost of the investigation. This project proposes an appropriate components of DF readiness for operational unit.

1.2 Problem Background

Any organization has critical information and sensitive information assets. In order to protect them from any threats or any attack must the organization must have a strategy in the workplace to ensure business continuity and maintain the confidentiality, integrity and availability of information.

According to (J. Barbara, 2005), if security auditors of the organization, after risk assessment, found that the risk is not high enough to mitigate, then it is regarded as acceptable or residual risk. The presence of residual risk is an important reason that motivates organizations have corporate forensics.

Organizations actually apply law forensic only a small percentage (less than 30%) of corporate security incidents (Peter, 2009). This shows that the plurality of the cases does not end up in court. However organizations need to study any violation of the corporate security that has taken place has been it having or not having legal implications. Consequently regardless, if these cases will or will not end up in court organizations have to investigate following a credible similar procedure. Due to need for compliance, legislative and other requirements there could not appropriate incident analysis of those cases other than digital forensic considerations.

(Casey, E. 2007) defined a digital forensic process as special procedure to be followed to investigate criminal activity digital and this procedure should be admissible in a court of law. Digital forensics is hard work, and thus cyber forensic experts need some methodologies to assist in the investigation of digital forensics. Each digital forensics investigation needs to follow the digital forensic investigation process.

Digital Forensics preserves the integrity of information and processes of the investigation and leads the organizations to link the attack to the attacker and preserve the evidence to take proper actions. This may or may not end successful in a court of law due to the related evidence can be impure by the staffs or the ICT infrastructure of the organization.

(CP Grobler, CP Louwrens, 2007) stated when security breaches occur, the organization will conduct digital forensic investigations. Digital Forensics has two methods to conduct it (proactive) and (reactive) incident.

In these days the investigations almost focus on reactive. Commonly the investigation relies on the law and legal enforcement aspects of an incident to determine the root-cause that bring the incident (Stephenson P, 2003). For example when the personal computer of a suspect has been seized, the hard drive is imaged and an investigation proceeds to search for traces of the evidence to ensure the admissibility of the evidence.

Forensic readiness is defined as "the ability of a corporate organization to maximize its potential to use digital evidence whilst minimizing the costs of the investigation" (Grobler, C Louwrens, 2007). DF readiness reduces interruption of the business processes whilst performing investigations. The DF readiness is essential for any organizations make them ready against any kind of attack. Also, forensic readiness produce a good plan for reducing the time and cost of investigation.

The lack of standards for compliance makes the implementation of Digital Forensic Readiness seems difficult, if not impossible in organizations (A. Mouhtaropoulos, M. Grobler, C.-T. Li, 2011). To prepare organizations for any incidents, the management of this organization must have the digital forensic readiness plans to mange policies and procedures.

1.3 Problem Statement

Currently, most organizations are implementing DF readiness to reduce the cost of an investigation. The DF readiness also provides the ability for organizations to collect and preserve digital evidences. Furthermore, it prepares the organization before an incident occurs. Unfortunately, there are some organizations neglect the importance of digital forensic readiness in their workplace. The problem statement in this project is that there is still no DF readiness for CICT in UTM. Therefore, the ability to implement and manage the DF readiness in an organization is seriously hampered. This research will focus on previous frameworks and comparison between the previous frameworks and analysis with the aim of combining and integrating the major components so as to come up with an appropriate components of DF readiness for CICT in UTM. The components will help managers and staff to comply with the digital forensics discipline in their organizations.

1.4 Project Objectives

The objectives of this project are:

- To assess and identify frameworks used to prepare organizations for digital forensic investigations.
- To propose DF readiness components.
- To evaluate and validate the DF readiness components.

1.5 Scopes of the Project

The scope that identifies the boundaries of the project listed below:

- Four existing digital forensics readiness frameworks.

- Proposing a DF readiness components for operational unit.
- The study will be conducted in CICT UTM as a case study.

1.6 The Significance Of The Project

The importance of this project is to contribute to the development of the digital forensics field and easy for business and IT managers to apply the DF readiness strategy to their organizations through the provision of an appropriate framework for compliance. Therefore, it is important to propose digital forensic readiness for operational unit.

1.7 Chapter Organization

This project includes six chapters. Chapter one presents the introduction, problem background, problem statement, Objectives, scopes and importance of this project. Chapter two discusses literature review and identifies the importance of digital forensics and digital forensic readiness for organizations. Besides that, chapter two discusses four essential frameworks and identifies and analyzes their components. Chapter three discusses the methodology used to conduct this project. Chapter four discusses the proposed framework for digital forensic readiness at CICT UTM. Chapter five discusses result of study. In the end, conclusion, recommendations and future work discuss in chapter six.

REFERENCES

A. Mouhtaropoulos, M. Grobler, and C.-T. Li, "Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives," in 2011 European Intelligence and Security Informatics Conference, 2011, pp. 191-196.

Carrier, B. D (2006). A Hypothesis-based Approach to Digital Forensic Investigations. *Cerias Tech Report 2006-06, Purdue University, Center for Education and Research in Information Assurance and Security*, West Lafayette

Carrier B, Spafford. E.(2003). Getting physical with the digital investigation process. *International journal of Digital Evidence*, vol. 2, no. 2.

Casey, E. (2007). Handbook of Computer Crime Investigation, Forensic Tools and Technology. *Elsevier Academic Press, San Diego USA.*

Cp Grobler, P. B. L.(2007). digital forensics: a multi-dimensional discipline.

Cp Louwrens, E. A. (2006). A control Framework for Digital Forensics. *in IFIP11.9 International Conference on Digital Forensics.* Orlando Florida: Springer.

D. Barske, A. Stander, J.Jordan (2010). A Digital Forensic Readiness Framework for South African SME's

Denis Trcˇek,, Habtamu Abie,smund Skomedal, and Iztok Starc (2010). Advanced Framework for Digital Forensic Technologies and Procedures.

CPNA (2005). AN INTRODUCTION TO FORENSIC READINESS PLANNING TECHNICAL NOTE . Centre for the Protection of National Infrastructure (CPNI).

Freiling, F. C., & Schwittay, B. (2007). A Common Process Model for Incident Response and Computer Forensics. *Proceedings of Conference on IT Incident Management and IT Forensics*. Germany.

Garcia J, (2006), Pro-Active and Re-Active Forensics, (September 5, 2006), http://jessland.net.

G. Pangalos, C. Iliousdis, I. Pagkalos (2010). the importance of corporate forensics readiness in information security framework

Grobler, C., C. Louwrens, And S.V. Solms. (2010). A framework to guide the implementation of Proactive Digital Forensics in organizations. *in Workshop for Digital Forensics* Krakow, Poland.

Grobler, C., C. Lowrens (2010). Digital Evidence Management Plan

Grobler, C., C. Louwrens (2007). Digital Forensics Readiness as a component of Information security.

J. Barbara, (2005). "Digital evidence accreditation in the corporate and business environment" *Digital Investigation Elsevier*, vol. 2, pp. 137-146

J. Forrester, A. B. I.(2007). A Digital Forensic investigative model for business organisations. *in IFIPSec*. Sandton.

J. Garcia. (2005), September). Proactive and reactive forensics. [Online].

Available: http://jessland.net./Docs.php

M. Grobler and I. Dlamini. (2010). managing digital evidence: the governance of digital forensics. Journal of Contemporary Management. [Online]. 7. Available: http://www.researchspace.csir.co.za

Peters, S. (2009). CSI Computer Crime and Security Survey. *Computer Security Institute.*

P, S.(2003). Conducting Incident Post Morterns. *Computer Fraud and Security*.

Rowlingson, R. (2004). A ten step Process for Forensic Readiness. *International journal of Digital Evidence*.

Ruan, K., Carthy, J.,Kechadi, T., Crosbie, M. (2011).'Cloud forensics: An overview' *Advances in Digital Forensics VI*

Sinangin, D.(2002). Computer Forensics Investigations in a Corporate Environment. *Computer Fraud and Security Bulletin,* 8.

Siti Rahayu Selamat, Robiah Yusof, Shahrin Sahib**,** Mapping Process of Digital Forensic Investigation Framework, *IJCSNS International Journal of Computer Science and Network Security,* VOL.8 No.10, October 2008.

TAntonio Pooe, L Labuschagne (2012). A conceptual model for digital forensic readiness.

Taylor, C., B. Endicott-Popovsky, And D.A. Frincke, Specifying digital forensics: A forensics policy approach. *Digital investigation, 2007. 4: p. 101-104.*

T.Weber, "Cybercrime threat rising sharply", BBC News website, in Davos, January 2009, available on line http://news.bbc.co.uk/2/hi/business/davos/7862549.stm.

Von Solms SH, Information Security: The Fourth Wave, Computers and Security, Volume 25, Issue3, May 2006, (Elsevier, 2006), p. 165-168.

Von Solms SH, Louwrens CP. Relationship between Digital Forensics, Corporate Governance, Information Technology and Information Security Governance , (Information Security Of South Africa Conference 2005 Proceeding, 2005).

Zavrsnik, A. (2008). Cybercrime definitional challenges and criminological particularities.