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.