UNIVERSITI TEKNOLOGI MARA

EMPLOYEES' PROTECTION MOTIVATION FOR ENHANCING CYBER SECURITY PROTECTIVE BEHAVIOUR

SAIF HUSSEIN ABDALLAH ALGHAZO

Thesis submitted in fulfilment
of the requirements for the degree of
Master of Science
Business and Management

Faculty of Business and Management

October 2024

ABSTRACT

In today's digital age, data and information are stored, used and processed online and in digital platforms. This results in creating tremendous challenges for corporation as well as individuals to ensure data and information are well protected to avoid any data breaches and cyber-attacks. This study focused on the managers' skills, protection motivation, countermeasure awareness in shaping cyber security protective behaviour among employees in the public sector corporations within the context of UAE. It proposes that Protection Motivation is driven by procedural information security countermeasures awareness (PCM) which also direct the cyber security protective behaviour (CPB). Further, the manager's Information Security Intelligence Skills (MISI) plays a crucial role towards CPB and PCM. To achieve this, the research followed quantitative cross-sectional and probability sampling to collect data from 520 employees and managers, and Partial least square structural equation modelling (PLS-SEM) for data analysis and hypothesis testing. The study finds that perceived threat susceptibility, self-efficacy, information security problem-solving, and social competence significantly affect cyber security protective behaviour. Additionally, managers' information security intelligence positively influences countermeasure awareness, which in turn affects cyber security protection motivation. Finally, attitude moderates the relationship between self-efficacy and cyber security protective behaviour. These findings offer valuable insights for organizations to enhance their cyber security practices and mitigate risks. The results are discussed, based on which, recommendations and implication are drawn at the end.

Keywords: Cybersecurity, Data Protection, Employee, Protection Behaviour, Motivation

ACKNOWLEDGEMENT

Firstly, I would forever be greatly indebted to the Almighty God who allowed me this opportunity and made it so that I am able to pursue my MSc and ensuring that I am able to successfully conclude this lengthy and challenging journey. I am also grateful and thankful to my supervisors Associate Professor Dr Norshima Binti Humaidi and Dr Nooriha Binti Abdullah.

I will forever be appreciative and grateful to the employees working with the organizations operating in the Abu Dhabi Public Sector, who took the time to respond to our survey questions that went a long way in helping us successfully assimilate and complete this research.

Finally, I would like to dedicate this thesis to my loving parents. I am forever grateful to my father and mother who had the sheer determination to provide me with quality education. This work of mine is dedicated to you. Thank you for always being there for me.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

Technological developments have seen a rapid evolution in the last decade. As technology evolves, business practices and methods have also drastically changed. In this direction, there have been remarkable changes in the way organizations carry out their businesses and the manner in which they store their data. With the evolution of technology, data storage methods have become so advanced that organizations prefer to store all their data digitally (Shaban et al., 2022), while data storage implies that it is properly organized and can be easily accessed anywhere and at any time, it also means that the data is more vulnerable (Mohammed, 2019). For instance, with more and more organizations choosing to store their data on the cloud, the need for cyber security awareness has become the need of the hour (Jang-Jaccard and Nepal, 2014). The sensitivity of the data stored in the cloud and the security measures taken to protect them become a pressing issue for all organizations who opt to store this data in the cloud.

With the rising need for cyber security, the demand for managers who are competent with dealing and handling this issue knowledgeably and efficiently is rising (Connolly and Wall, 2019). The manager's competency and awareness of the problem become a deciding factor in determining how they handle the situation and their response. It also determines the measures taken up by them to protect the data they have been entrusted with. One of the essential skills for managers is the managers' information security intelligence (MISI) competencies, in which managers with MISI competencies exhibit familiarity with wide range of information security skills such as security and network architectures, systems and frameworks, and compliance related skills.

Intelligence skills necessary for the security of information and the protection motivation for cyber security behaviour become an essential competency for managers to ensure the safety of this data (Campbell, 2017). This study aimed to evaluate how these competencies affect how organizations handle information security programs in