FACTORS INFLUENCING CYBERSECURITY PERFORMANCE MEDIATED BY CYBERSECURITY READINESS IN PUBLIC ORGANIZATIONS OF UAE

SULAIMAN MOHAMMED SULAIMAN ALSAGHER ALSHEMILI

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DOCTOR OF PHILOSOPHY

2023

Institute of Technology Management and Entrepreneurship

FACTORS INFLUENCING CYBERSECURITY PERFORMANCE MEDIATED BY CYBERSECURITY READINESS IN PUBLIC ORGANIZATIONS OF UAE

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

SULAIMAN MOHAMMED SULAIMAN ALSAGHER ALSHEMLI

Doctor of Philosophy

2023

FACTORS INFLUENCING CYBERSECURITY PERFORMANCE MEDIATED BY CYBERSECURITY READINESS IN PUBLIC ORGANIZATIONS OF UAE

SULAIMAN MOHAMMED SULAIMAN ALSAGHEER ALSHEMILI

A thesis submitted
in fulfillment of the requirements for the degree of
Doctor of Philosophy

Institute of Technology Management and Entrepreneurship

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I declare that this thesis entitled “Factors Influencing Cybersecurity Performance Mediated by Cybersecurity Readiness in Public Organization of UAE” is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature	:	*Sulaiman AlShemili*
Name	:	Sulaiman Mohammed Sulaiman Al Shagheer AlShamili
Date	:	15 May 2023

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

APPROVAL

I hereby declare that I have read this thesis and in my opinion, this thesis is sufficient in terms of scope and quality for the award of the degree of. Doctor of Philosophy.

Signature : 

Supervisor Name : Assoc. Prof. Dr. Safiah Sidek

Date : 20 May 2023

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DEDICATION

I would like to dedicate my highest acknowledgement to my beloved family for always being with me through all the hardship of my study by giving consistently support and encouragement.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ABSTRACT

The increasing digitization of services and operations in the United Arab Emirates (UAE) has necessitated an urgent need to understand the factors that influence cybersecurity readiness and its subsequent impact on cybersecurity performance. As the UAE has become one of the most targeted nations for cybercrime, effective strategies to combat these threats have become critical. Further, based on a preliminary study, it was found that despite the high levels of readiness and performance in certain aspects, there are notable shortcomings, particularly in organizational readiness and the awareness of organizational security. This context, coupled with the findings of the preliminary study highlight the urgent need for a research on cybersecurity readiness in UAE public organizations. This study seeks to identify the key factors that contribute to cybersecurity readiness and how they subsequently affect cybersecurity performance within organizations in the UAE. Specifically, framed by Technology-Organization-Environment (TOE) Framework, this study examined the influence of IT infrastructure, employees' skills, top management support, government regulations, government support, and industry standards on cybersecurity readiness and performance. Data were collected from 238 employees of the three largest public organizations in Abu Dhabi and analysed using the Partial Least Squares Structural Equation Modelling (PLS-SEM) approach. The findings revealed that IT infrastructure, employees' skills, top management support, and government regulations significantly influence cybersecurity readiness, which in turn impacts cybersecurity performance. While government support was found to significantly influence organizational cybersecurity performance, it did not significantly influence cybersecurity readiness. Industry standards significantly affected cybersecurity readiness but did not have a significant impact on organizational cybersecurity performance. Cybersecurity readiness was found to mediate the relationships between IT infrastructure, employees' skills, top management support, government regulation, industry standards and cybersecurity performance. However, it did not mediate the relationship between government support and cybersecurity performance. The study highlights the importance of a multifaceted approach towards enhancing cybersecurity readiness and performance in organizations, thereby contributing to a safer and more secure digital environment in the UAE. These findings carry significant implications for policy makers, regulators, and organizational leaders, emphasizing the need for a comprehensive strategy involving robust IT infrastructure, skilled workforce, supportive management, effective regulations, and adherence to industry standards, complemented by a strong focus on enhancing cybersecurity readiness. It paves the way for strategic decision-making and effective interventions that not only maintain but further enhance the country's cybersecurity readiness and performance, thereby strengthening its resilience against an evolving cyber threat landscape.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

FAKTOR YANG MEMPENGARUHI PRESTASI SEKURITI SIBER DIMEDIASI OLEH KESEDIAAN SEKURITI SIBER DI ORGANISASI AWAM UAE

ABSTRAK

Peningkatan digitalisasi perkhidmatan dan operasi di Emiriah Arab Bersatu (UAE) telah menuntut keperluan mendesak untuk memahami faktor-faktor yang mempengaruhi kesediaan keselamatan siber dan kesan berikutnya terhadap prestasi keselamatan siber. Seiring dengan UAE menjadi salah satu negara paling disasarkan untuk jenayah siber, strategi berkesan untuk memerangi ancaman-ancaman ini telah menjadi kritikal. Selanjutnya, berdasarkan kajian awal, didapati bahawa meskipun terdapat tahap kesediaan dan prestasi yang tinggi dalam aspek tertentu, terdapat kekurangan yang ketara, terutama dalam kesediaan organisasi dan kesedaran keselamatan organisasi. Konteks ini, ditambah dengan penemuan kajian awal menunjukkan keperluan mendesak untuk menjalankan kajian tentang kesediaan keselamatan siber dalam organisasi awam UAE. Kajian ini bertujuan mengenal pasti faktor-faktor utama yang menyumbang kepada kesediaan keselamatan siber dan bagaimana faktor-faktor ini seterusnya mempengaruhi prestasi keselamatan siber dalam organisasi di UAE. Berpandukan kepada Kerangka Teknologi-Organisasi-Persekitaran (TOE), kajian ini mengkaji pengaruh infrastruktur IT, kemahiran pekerja, sokongan pengurusan atasan, peraturan kerajaan, sokongan kerajaan, dan piawaian industri terhadap kesediaan dan prestasi keselamatan siber. Data dikumpulkan dari 238 pekerja di tiga organisasi awam terbesar di Abu Dhabi dan dianalisis menggunakan pendekatan Model Partial Least Squares (PLS-SEM). Penemuan menunjukkan bahawa infrastruktur IT, kemahiran pekerja, sokongan pengurusan atasan, dan peraturan kerajaan mempengaruhi kesediaan keselamatan siber secara signifikan, yang seterusnya memberi kesan kepada prestasi keselamatan siber. Walaupun sokongan kerajaan didapati memberi pengaruh signifikan terhadap prestasi keselamatan siber organisasi, ia tidak memberi pengaruh signifikan terhadap kesediaan keselamatan siber. Piawaian industri memberi kesan signifikan terhadap kesediaan keselamatan siber tetapi tidak memberi kesan signifikan terhadap prestasi keselamatan siber organisasi. Kesediaan keselamatan siber didapati memediasi hubungan antara infrastruktur IT, kemahiran pekerja, sokongan pengurusan atasan, peraturan kerajaan, piawaian industri dan prestasi keselamatan siber. Walau bagaimanapun, kesediaan keselamatan siber tidak memediasi hubungan antara sokongan kerajaan dan prestasi keselamatan siber. Kajian ini menekankan kepentingan pendekatan pelbagai aspek terhadap peningkatan kesediaan dan prestasi keselamatan siber dalam organisasi, dengan ini menyumbang kepada persekitaran digital yang lebih selamat dan lebih terjamin di UAE. Penemuan ini membawa implikasi signifikan bagi pembuat dasar, pengawal, dan pemimpin organisasi, menekankan keperluan strategi komprehensif yang melibatkan infrastruktur IT yang kukuh, tenaga kerja yang berkemahiran, pengurusan yang menyokong, peraturan yang berkesan, dan pematuhan terhadap piawaian industri, disertai dengan tumpuan kuat terhadap peningkatan kesediaan keselamatan siber. Ia juga membuka jalan untuk pembuatan keputusan strategik dan intervensi berkesan yang bukan sahaja mengekalkan tetapi juga meningkatkan kesediaan dan prestasi keselamatan siber negara, dengan itu meningkatkan daya tahan terhadap lanskap ancaman siber yang berkembang.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful

First and foremost, I would like to thank my main supervisor, Assoc. Prof. Dr. Safiah Sidek for the continuous support of my PhD study and related research, for her patience, motivation, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I would also like to express my greatest gratitude to all the lecturers in UTeM on their willingness to help me out in this research. They are always open whenever I ran into a trouble spot or had a question about my research or writing. Special gratitude also for my colleagues in UTeM and my workplaces for supporting me through their encouragement and honest comment on my research

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

TABLE OF CONTENTS

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF TABLES

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF FIGURES

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF SYMBOLS

R^2	-	Coefficient of determination value
f^2	-	Effect size

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF ABBREVIATIONS

IEC	-	International Electrotechnical Commission
ISO	-	International Organization of Standardization
ICT	-	Information and Communication Technology
IT	-	Information Technology
PMT	-	Protection Motivation Theory
NIST	-	National Institute of Standards and Technology
RBV	-	Resource-based View
SCT	-	Social Cognitive Theory
TAM	-	Technology Acceptance Model
TRA	-	Theory of Reasoned Actions
TOE	-	Technology-Organization-Environment
UAE	-	United Arab Emirates

UTeM
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF APPENDICES

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF PUBLICATIONS

The followings are the list of publications related to the work on this thesis:

Mohammed, S., Kamalrudin, M., Al-Shami, S. A., Hakimi, H., and Sidek, S., 2020. Cybersecurity readiness model of public organizations: Conceptual framework. *Test Engineering and Management,* 83, pp. 13548-13558.

Mohammed, S., Kamalrudin, M., Al-Shami, S.A., Hakimi, H., and Sidek, S., 2019. A Study on Readiness Model of Public organizations. *International Journal of Recent Technology and Engineering (IJRTE),* 8 (1C2), pp. 851-856.

UTeM
اونيۏرسيتي تيکنيکل مليسيا ملاک
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

CHAPTER 1

INTRODUCTION

This study seeks to investigate the relationship between cybersecurity readiness and the security performance among employees in the public organizations. Considering the high rates of cybercrimes globally due to the increasing usage of digital technologies in the business and daily practices, it is crucial to find ways to provide a secure and safe cyber space for everyone. In a similar vein, public organizations, which are increasingly using digital technologies for the provision of the public services are also threatened with cybercrimes. Hence, it is vital to ensure that employees of the public government are ready and equipped with the necessary security practices so that they can provide safe and secured services. Advocating that developing security readiness among users may contribute to the provision of secure and safe cyber space, this study aims to propose a cybersecurity readiness model that contributes to the security performance of employees in public organizations. It is expected that the security practices among employees of public organization facilitate the provision of effective and efficient public services for the development of a digitally safe environment country.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

This chapter is an introductory chapter that consists of seven sections. The first section provides the background of the research, which is followed by the problem statement addressed in this research. The third and fourth section outline the research objectives and research questions of this research. Next, the fifth section presents the scope of the research, followed by the sixth section that presents the contribution of this research. The seventh section presents the operational definition of the constructs involved in this research. This chapter ends with the organization of the thesis

1.1 Background

This section provides the background of the research, highlighting the need for cyber security awareness model in response to the increasing trend of cybercrimes. This research is contextualized within the socio-economic background of the UAE. For this purpose, this section is organized into two subheadings: The first sub-heading focuses on the increasing trend of cybercrimes, while the second sub-heading presents a preliminary study of the issues related to the cybersecurity awareness in the UAE.

1.1.1 Digitalization and cybercrimes

Cyberspace has become an essential part in everyone's live, including the provision of business transactions and public services (Alwasmi, 2022). Many have claimed that the impetus of the increasing activities in the digital world is due to the continuous advancement in Information Communication Technology coupled with the development of big data, automation and Internet of Things (IoT) (Younies and Na, 2020). This trend has resulted in a dynamic economy that allows borderless information and media sharing (Alwasmi, 2022).

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Similarly, the transformation of the public organizations towards digitalization, namely their transformation towards e-government, mobile government or smart government has resulted in the heavily usage of digital technologies in almost all activities in the government. Public organizations (such as any municipal government, public authority, state agency, or other governmental unit) are non-profit economic development organizations that have significant role for the growth of the nation (Wang, 2022). In this respect, employees in the public organization do not have much choice, but to depend on the digital technologies to perform their work

However, the global penetration of the Internet and the rising number of internet users has led to an exponential increase in opportunities of cybercrime (Rajan, Ravikumar

and Al Shaer, 2017; Younies and Na, 2020; Phillips, Davidson, Farr, Burkhardt, Caneppele and Aiken, 2022). Cybercrime generally refers to any criminal act dealing with computers, networks and hardware device and it has become a pervasive in modern life. Based on a survey on global economic crime and fraud survey conducted by Pricewater House Company, which collected the views of almost 1,300 executives across 53 countries, it was found that cybercrime is the biggest fraud threat faced by most businesses today (PwC's Global Economic Crime and Fraud Survey, 2022). It was also reported that four in ten organization experienced some forms of fraud connected to digital platforms such as data breaches, disinformation, money laundering, terrorism financing and many others. In this regard, despite the benefits facilitated by the advanced development in digital technologies, individuals, especially businesses are increasingly facing with cybercrime. In relation to this, cybersecurity policies and practices are more vital than ever (Wandkhede and Vinodh, 2022).

Cybercrimes have become serious threats for not only the individuals, organization and enterprises, but also the public organizations (Vlachos, Minou, Assimakopous and Toska, 2014; Giri, 2019; Donalds and Osei-Bryson, 2019; Kagita, Thilakarathne, and Gedekallu, 2021). Further, the costs and impacts of cybercrimes has been substantial for both the public or private organizations (Hasan, Ali, Kurnia and Thurasamy, 2021). Morgan (2020) asserted that cybercrime damage costs were estimated to hit US$ 6 trillion annually in 2021. The increasinlgy incidence of cybercrime indicate the importance of paying attention to cybersecurity.

Although digitalization is expected to improve the efficiency and effectiveness of public administration and the provision of public services, the public sectors are also vulnerable to cybercrimes (Oni, Berepubo, Oni, and Joshua, 2019). In fact, public organizations have been identified as among the top industries that experience cyber attacks

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

(Symantec, 2015). The lack of preparation for security measures in the operations of the organizations may disrupt the effectiveness and efficiency of the organization. The security vulnerabilities in public organizations may lead to severe consequences for individuals, companies, administraton, and government (Wirtz and Weyerer, 2016).

Cheang (2009) highlighted the importance of 'peopleware' for tackling cybercrimes since the crimes are man-made. Hence, it is very important to ensure that the employees of the public organizations are ready with the necessary knowledge and skills to protect their work against cybercrimes. In this case, cybersecurity measures need to be emphasized in the public organizations to ensure the organizations are working in an environment protected from cybercrimes. By doing so, these organizations will be able to perform effectively and efficiently for the development of the countries and nation.

In general terms, cybersecurity refers to the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve it (Oxford University Press, 2014). It is the protection of an organization's computer systems against theft, damage to hardware or electronic data, and interruption or diversion of services (Kasperksy Lab, 2019). Taking this into account, the biggest threats facing companies in cybersecurity are related to data breaches, that can lead to unauthorized access or disclosure of sensitive, confidential, or other protected data (Von Solms and Von Solms, 2018).

Meanwhile, cybersecurity readiness refers to the ability of an organization to effectively detect and respond to computer cyber–security intrusions and breaches, theft of data and intellectual property, phishing attacks, and malware attacks from both outside and inside the network (Sullivan, 2016). In this case, organizations should focus on their preparedness and response cabilitilies rather than soley trying to prevent cyber attacks. In other words, organizations should emphasize on proactive cybersecurity measures and incident response planning to mitigate the impact of cyberattacks. Many cybersecurity

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

resources and guides, such as the NIST Cybersecurity Framework emphasize the need for organizations to prepare for cyber incidents rather than simply hoping to avoid them altogether. Therefore, it is crucial for organizations to establish sufficient level of cybersecurity readiness for better financial returns, improved reputation and superior firm performance (Smith, Winchester, Bunker and Jamieson, 2010; Tsou and Hsu, 2015; Smith, Dhillonn and Carter, 2021).

1.1.2 A preliminary study: Cybersecurity performance in the UAE

The UAE has become the chief target of cybercriminal activities due to the higher economic activities and level and tourism, significant uptake of technology and the rise of the oil and gas (Rajan et al., 2017). A research conducted by Alwasmi (2022) showed that there is a relative difference between the cybercriminal activity in the UAE and globally. In this regard, it has been noted that cybercrimes have been rising, and governments are introducing newer policies, reforms, and measures for all cybercriminal activities. In a similar context, Younies and Na (2020) explored the extent to which cybercrime laws protect citizens and businesses in the United Arab Emirates (UAE). It was found that the UAE has taken decisive and proactive measures to deter the threat of cybercrimes and cyberattacks. Although the UAE has comprehensive cybercrime laws, the remarkable level of technological advances in the country makes citizens and businesses lucrative targets for cybercriminals (Younies and Na, 2020). As such, a research focusing on the effects of cybersecurity awareness on performance is still relevant in the UAE.

To support the claim that there is a need to propose a cybersecurity readiness model for public organizations, a preliminary of the issues and challenges related to cyber securities in the UAE has been conducted. The purpose of the preliminary study was to identify the

UNIVERSITI TEKNIKAL MALAYSIA MELAKA