UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DETERMINANTS OF CYBERATTACK PREVENTION AND THE ROLE OF CYBERSECURITY LEADERSHIP IN UAE BANKING SECTOR

SULTAN KHALIFA HUMAID KHALIFA ALSHAMSI

DOCTOR OF PHILOSOPHY

2023

Faculty of Technology Management and Technopreneurship

DETERMINANTS OF CYBERATTACK PREVENTION AND THE ROLE OF CYBERSECURITY LEADERSHIP IN UAE BANKING SECTOR

Sultan Khalifa Humaid Khalifa Alshamsi

Doctor of Philosophy

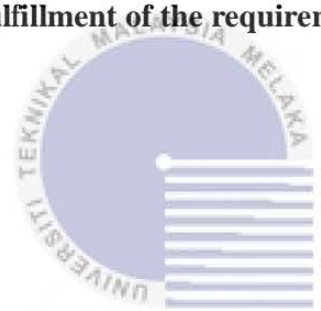
2023

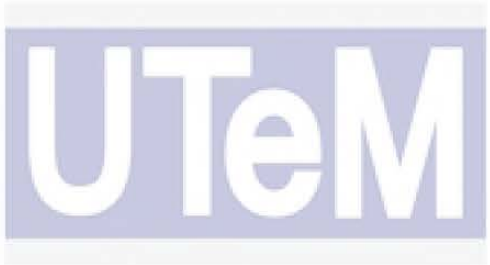
DETERMINANTS OF CYBERATTACK PREVENTION AND THE ROLE OF CYBERSECURITY LEADERSHIP IN UAE BANKING SECTOR

SULTAN KHALIFA HUMAID KHALIFA ALSHAMSI

A thesis submitted

in fulfillment of the requirements for the degree of Doctor of Philosophy





Faculty of Technology Management and Technopreneurship

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I declare that this thesis entitled "Determinants of Cyberattack Prevention among Individuals in UAE Financial Organizations" 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 : .....

Name : Sultan Khalifa humaid khalifa alshamsi

Date : 20 / 8 / 2023

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 Doctor of Philosophy.

Signature : .....

Supervisor Name : Nabil Hasan Saleh Al-kumaim

Date : 25 / 8 / 2023

DEDICATION

I want to dedicate this thesis to my cherished parents and my family, who have inspired me and given me strength. Without their ongoing moral, spiritual, and financial support, there is little question that I would not have finished this work.

ABSTRACT

Today's organized criminal groups focus on easy ways to make money, ways that target rich organizations because a large amount of money flows daily and contains sensitive information. Cyberattack prevention factors have a significant impact on the perception of social and moral values in the business context. Moreover, cyberattacks have become a crucial matter among world's developed countries as well as developing countries like UAE. Therefore, there is a need to study the role of skilled leaders in financial organizations in the UAE in preventing cyberattacks and investigate other human factors related to the individual in financial organizations in UAE in preventing cyberattacks. A general perception of the research is to propose a research framework for cyberattack prevention in the UAE by employing the Protection Motivation Theory and adding new variables focusing on the role of an organization's cybersecurity leadership, frequent training, and the role of government frequent alerting. A proposed framework and 22 hypotheses were constructed to guide this study. This research employed a quantitative research method. The data were collected from 310 financial executive officers from a commercial bank in the Central Bank, an industrial bank in the Emirates Industrial Bank, a merchant bank in the Ajman Bank, and an Islamic bank in the ADIB bank of the UAE that use digital technology to enhance their daily banking operation through survey questionnaires. Subsequently, the data were analyzed using Structural Equation Modelling (SEM) as a statistical methods and techniques approach. The results indicated a significant association between all investigated independent variables and cybersecurity leadership, and cybersecurity leadership mediates the relationship between investigated independent variables and cyberattack prevention. No significant association was shown between investigated independent variables and cyberattack prevention, except (H4&H7) that show a significant association. Although UAE government regularly applies and invests in many technical measures to prevent cyberattack in both individual and organizational levels, many UAE financial firms have been identified as high-level targets in cyberattacks in this digital transformation era. The coefficient in cybersecurity leadership might be viewed as a prevention element for cyberattacks based on the findings. With greater cybersecurity leadership success, the implementation of cyberattack prevention increases. This study emphasizes the importance of cybersecurity leadership in a cyberspace environment that protects against cyberattacks and promotes cybersecurity awareness within a financial organizations and society in UAE. The research framework contributes to the development of cyberattack prevention by encouraging cybersecurity leadership in setting cybersecurity strategy, positioning cybersecurity functions, and implementing cybersecurity activities through protection motivation theory that emphasizes (1) threat appraisal that guarantees security guidelines are reasonable and seen for the organizational climate and (2) coping appraisal that guarantees threat data is joined by useful data in deferring it, which is appropriate for this research setting in a banking climate, (3) leadership's important role in leveraging and fostering cyberattack prevention in UAE financial sector.

PENENTU PENCEGAHAN SERANGAN SIBER DAN PERANAN KEPIMPINAN KESELAMATAN SIBER DALAM SEKTOR PERBANKAN UAE

ABSTRAK

Kumpulan penjenayah terancang hari ini memberi tumpuan kepada cara mudah untuk membuat wang yang menyasarkan organisasi kaya kerana sejumlah besar wang mengalir setiap hari dan mengandungi maklumat sensitif. Faktor pencegahan serangan siber mempunyai kesan yang besar terhadap persepsi nilai sosial dan moral dalam konteks perniagaan. Lebih-lebih lagi, serangan siber telah menjadi perkara penting di kalangan negara maju di dunia serta negara membangun seperti UAE. Oleh itu, terdapat keperluan untuk mengkaji peranan pemimpin mahir dalam organisasi kewangan di UAE dalam mencegah serangan siber dan menyiasat faktor manusia lain yang berkaitan dengan individu dalam organisasi kewangan di UAE dalam mencegah serangan siber. Persepsi umum penyelidikan adalah untuk mencadangkan rangka kerja penyelidikan untuk pencegahan serangan siber di UAE dengan menggunakan Teori Motivasi Perlindungan dan menambah pembolehubah baharu yang memfokuskan pada peranan kepimpinan keselamatan siber organisasi, latihan yang kerap dan peranan amaran kerajaan yang kerap. Satu rangka kerja yang dicadangkan dan 22 hipotesis telah dibina untuk membimbing kajian ini. Penyelidikan ini menggunakan kaedah kajian kuantitatif. Data tersebut dikumpul daripada 310 pegawai eksekutif kewangan dari sebuah bank komersial di Bank Pusat, sebuah bank perindustrian di Emirates Industrial Bank, sebuah bank saudagar di Ajman Bank, dan sebuah bank Islam di bank ADIB UAE yang menggunakan teknologi digital untuk meningkatkan operasi perbankan harian mereka melalui soal selidik tinjauan. Selepas itu, data dianalisis menggunakan Pemodelan Persamaan Struktur (SEM) sebagai kaedah statistik dan pendekatan teknik. Keputusan menunjukkan hubungan yang signifikan antara semua pembolehubah bebas dan kepimpinan keselamatan siber yang disiasat, dan kepimpinan keselamatan siber menjadi pengantara hubungan antara pembolehubah bebas yang disiasat dan pencegahan serangan siber. Walaupun tidak ada kaitan yang signifikan antara pembolehubah bebas yang disiasat dan pencegahan serangan siber, kecuali (H4 &H7) yang menunjukkan perkaitan yang signifikan. Walaupun, kerajaan UAE kerap memohon dan melabur dalam banyak langkah teknikal untuk mencegah serangan siber di peringkat individu dan organisasi, namun banyak firma kewangan UAE telah dikenal pasti sebagai sasaran peringkat tinggi dalam serangan siber dalam era transformasi digital ini. Pekali dalam kepimpinan keselamatan siber mungkin dilihat sebagai elemen pencegahan serangan siber berdasarkan penemuan tersebut. Dengan kejayaan kepimpinan keselamatan siber yang lebih besar, pelaksanaan pencegahan serangan siber meningkat. Kajian ini menekankan kepentingan kepimpinan keselamatan siber dalam persekitaran ruang siber yang melindungi daripada serangan siber dan mempromosikan kesedaran keselamatan siber dalam organisasi kewangan dan masyarakat di UAE. Rangka kerja penyelidikan menyumbang kepada pembangunan pencegahan serangan siber dengan menggalakkan kepimpinan keselamatan siber dalam menetapkan strategi keselamatan siber, meletakkan fungsi keselamatan siber, dan melaksanakan aktiviti keselamatan siber melalui teori motivasi perlindungan yang menekankan (1) penilaian ancaman yang menjamin garis

panduan keselamatan adalah munasabah dan dilihat untuk iklim organisasi dan (2) mengatasi penilaian yang menjamin data ancaman disertai oleh data berguna dalam menangguhkannya, yang sesuai untuk suasana penyelidikan ini dalam iklim perbankan, (3) peranan penting kepimpinan dalam memanfaatkan dan memupuk pencegahan serangan siber dalam sektor kewangan UAE.

ACKNOWLEDGEMENTS

My supervisor, Dr. Nabil Hasan Saleh Al-Kumaim, guided me and provided me with consistent assistance while I finished my thesis, and for that, I wish to convey my sincere gratitude. Her encouragement and support have helped me to approach finishing my thesis with a positive outlook, and I am grateful for that.

I'm grateful to my wife, kids, and parents for their support, prayers, unending tolerance, and for helping me prepare for the future by helping me finish my research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AVE	-	Average Variance Extracted
CBUAE	-	Central Bank UAE
CFA	-	Confirmatory Factor Analysis
CL	-	Cyberattack Prevention
CP	-	Cybersecurity Leadership
CR	-	Composite Reliability
EFA	-	Exploratory Factor Analysis
GF	-	Government Frequent Alerting
ICA	-	Implement Cybersecurity Activities
IC	-	Internal Consistency
IR	-	Indicator Reliability
NGO	-	Non-Governmental Organizations
OFT	-	Organization Frequent Training
PLS	-	Partial Least Squares
PSF	-	Position Cybersecurity Functions
PS	-	Perceived Severity
PV	-	Perceived Vulnerability
RC	-	Response-Cost
RE	-	Response-Efficacy
SCS	-	Set Cybersecurity Strategy
SD	-	Standard Deviation

SE	-	Self-Efficacy
SEM	-	Structural Equation Modelling
SPSS	-	Statistical Package for Social Science
TDRA	-	Telecommunications and Digital Government Regulatory Authority
UAE	-	United Arab Emirates
NESA	-	National Electronic Security Authority
DESC	-	Dubai Electronic Security Center
ADDA	-	Abu Dhabi Digital Authority
VAF	-	Variance Accounted For
VIF	-	Variance Inflation Factor

LIST OF APPENDICES

LIST OF PUBLICATIONS

1. *Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership - NH Al-Kumaim, SK Alshamsi. Applied Sciences 13 (10), 5839*

2. *Sultan Khalifa Humaid Khalifa Alshamsi and Al-kumaim, N.H.S., 2021. A conceptual model for prevention of e-financial crimes in UAE: a review paper. Academic of Strategic Management Journal, 20(Special Issue 6), pp.1–11.*

CHAPTER 1

INTRODUCTION

1.1 Introduction

A general perception of this research is to propose a research framework for cyberattack prevention in the UAE Financial organizations, mainly banks, by employing the Protection Motivation Theory (PMT) and adding new variables focusing on the role of an organization's cybersecurity leadership, frequent training, and the role of government frequent alerting. This chapter presents the background of the research, research problems, research objectives, and research questions. Furthermore, the significance and scope of the research are determined to implement the research properly.

1.2 Background of the problem

Cyberattacks are criminal activity that utilizes electronic cracking that attacks organizations (Herath et al., 2018). Moreover, cyberattacks have become a crucial matter among the worlds' developed countries as well as developing countries like UAE (Halbouni et al., 2016). According to Zaabi and Awamleh (2019), the United Nations Crime Trends for 2019 showed that UAE ranked 36th out of 180 countries in the world for higher cyberattacks, as shown in Figure 1.1.

E-CRIME PERCEPTIONS INDEX 2019
- MUSLIM COUNTRIES

UNODC

Country	2018 Score	2018 Rank	2019 Score	2019 Rank
UAE	71/100	21/180	75/100	36/180
Qatar	63	29	62	33
Brunei	62	32	63	31
Jordan	48	59	49	58
Saudi Arabia	57	49	58	49
Oman	68	44	52	53
Malaysia	47	62	47	61
Indonesia	37	96	38	89
Egypt	32	117	35	105
Pakistan	32	117	30	117
Yemen	16	175	14	176

Figure 1.1: The United Nations Crime Trends for 2019, Source: United Nations Office on Drugs and Crime Report (2019)

Moreover, the UAE scored 56% on worldwide cyberattack levels (Gibbs, 2018). Cyberattacks raise complex issues with new technologies that brought unprecedented threats to social problems for UAE (Yacoubi, 2020). Cyberattacks have major impacts on a wide variety of public safety where it reduces confidence in personal identity and computer security (Kuru and Bayraktar, 2017), national security impact through reduction in economic strength (Lemieux, 2018), and human security that creates danger and fear for an individual (Barrera, 2019).

In the UAE, cyberattacks are focused on phishing and fraud which emphasize a rapidly growing online base (Ferguson et al., 2020). General Department of Criminal Investigation, Department of E-Investigation UAE Police statistics reveal a 46% increase in crimes involving identity theft (Afifi, 2019). The UAE Police statistics showed that in 2019, there were 9046 complaints with 1277 coming from social media accounts that had been hacked (Zabyelina, 2019). Most of these cases were filed by women that belong to wealthy,

educated, and government officers' families that were blackmailed through cyberattacks (Mahdavi, 2019).

Today's organized criminal groups focus on easy ways to make money, ways that target rich organizations because a large amount of money flows daily and contains sensitive information (Ratten, 2019). Therefore, the organization encounters cyberattack problems through hacking, malicious software, and identity theft which occurs due to the complexity of technology (Nowacki and Willits, 2019). Moreover, data breaches occur due to the digitization of data storage that stored private data and records which consist of confidential information and financial progress (Weijer et al., 2020).

Organized criminal groups are gradually moving toward damaging the reputation of the business through hacking the networks that contain business-sensitive information which may cost greater loss to the business performance (Malik and Islam, 2019). Moreover, this problem occurs due to the adoption of modern technology that consists of information flow, which has no boundary and is difficult to be monitored (Torre et al., 2018). Furthermore, borderless transfer of technology is exposed to new ways of theft in the data breach that negatively affects the organization (Arewa, 2018).

Cyberattack prevention factors have a significant impact on the perception of social and moral values in the business context. However, the causes behind cyberattacks are complicated to be eliminated because they are mapped to electronic criminality that keeps on growing (Koziarski and Lee, 2020). Moreover, the cyberattack has a bad impact on the business context because unauthorized access consists of many possibilities of a data breach due to complex technology (Shah et al., 2019).

Furthermore, cyberattack also gives a macroeconomic impact that leads to a stronger international competition which significantly reduced revenues from local organization taxes and social infrastructure (Teichmann and Falker, 2020). Yet, cyberattacks will