UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Faculty of Information and Communication Technology

INFORMATION SECURITY BEHAVIOUR ASSESSMENT IN SOFTWARE-AS-A-SERVICE CLOUD ENVIRONMENT

Hanifah binti Abdul Hamid

Doctor of Philosophy

2018

INFORMATION SECURITY BEHAVIOUR ASSESSMENT IN SOFTWARE-AS-A-SERVICE CLOUD ENVIRONMENT

HANIFAH BINTI ABDUL HAMID

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

Faculty of Information and Communication Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2018

DECLARATION

I declare that this thesis entitled "Information Security Behaviour Assessment in Software-as-a-Service Cloud Environment" 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	:	HANIFAH BINTI ABDUL HAMID
Date	:	25/10/2018

APPROVAL

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

Signature : ....

Supervisor Name : DR. ZERATUL IZZAH BINTI MOHD YUSOH

Date : 25/10/2018

DEDICATION

To my beloved husband, parents and children

ABSTRACT

This research aims at assessing the information security behaviour in Software as a Service (SaaS) cloud computing environment. Organisations are still struggling with information security breaches despite various technical protections to secure SaaS applications. This is due to the fact that human behaviour is the weakest link of the security chain. Security compromise causes substantial financial and nonfinancial losses to the organisations which jeopardise organisations' reputation. Technical protection alone is seemed insufficient to ensure information safety. Therefore, this research takes it from the socio-organisational perspective to strengthen information security. Many socio-organisational factors influence employees' security behaviour in the organisation which gives impact to SaaS cloud adoption. Addressing these factors are significant to help successfully create a healthy security culture in the organisation. Nevertheless, human behaviour is subjective in nature. Their behaviour depends upon the way they think feel and act towards security issues which needs an in depth understanding towards their security behaviour. Hence, adapting the sequential exploratory mixed-method approach, through the theoretical lens of social cognitive theory, organisational culture theory as well as security control from extended deterrence theory, this study develops an information security behaviour model and validates the socio-organisational aspects of security behaviour. There were 396 useful data gathered from the survey. SPSS 20 and PLS-SEM software were utilised for descriptive and exploratory factor analysis respectively. The survey results indicate that the security control management, personal values and behaviour were salient factors towards formation of good security behaviour. This research subsequently conducted a case study using the proposed model at one information technology department in a public university. The survey obtained 90 useful data. The case study revealed that organisational security culture, personal values as well as behaviour have significant influence towards information security behaviour. There were slight differences in the quantitative results to which the follow-up interview with three informants supported the findings from the case study. It can be concluded that personal values and behaviour elements are the most significant factors which influence information security behaviour of employees working in SaaS cloud environment. However, the organisation culture and security control management factors are observed to be contextually dependent as these factors depend on how the organisation is run by the respective top management. This study contributes both theoretically and practically. The information security behaviour's body of knowledge is built up through conceptual model testing and accentuating new propositions. The information security behaviour model was developed upon the integration of social cognitive theory, Wallach Organisational Culture Model as well as security control management from extended deterrence theory, and validated through a survey and a case study. The result helps the researcher to have better insight of employees' security behaviour in SaaS cloud environment in Malaysia generally and at the studied IT department specifically. The developed model, new accentuated propositions and other recommendations in this research may help other researchers to embark on related studies in the future.

ABSTRAK

Kajian ini bertujuan untuk menilai tingkah laku keselamatan maklumat di dalam konteks persekitaran perkomputeran awan Dewasa ini organisasi masih lagi berhadapan dengan cabaran kebocoran maklumat walaupun mempunyai pelbagai perlindungan teknikal bagi memastikan keselamatan aplikasi SaaS yang digunakan. Ini kerana tingkah laku pekerja-pekerja itu sendiri yang merupakan titik paling lemah dalam rantaian keselamatan maklumat. Keselamatan maklumat yang terjejas menyebabkan kerugian kewangan dan bukan kewangan yang besar kepada organisasi. Perlindungan teknikal sahaja seperti tidak mencukupi untuk memastikan keselamatan maklumat. Oleh itu, kajian ini menggunakan perspektif sosio-organisasi untuk memperkukuhkan keselamatan maklumat. Faktor sosio-organisasi banyak mempengaruhi kelakuan keselamatan pekerja dalam organisasi yang juga memberi kesan kepada perkembangan penggunaan perkomputeran awan. Menangani faktor kritikal ini adalah penting untuk membantu mewujudkan budaya keselamatan yang sihat dalam organisasi. Walau bagaimanapun, perlakuan manusia adalah bersifat subjektif bergantung kepada cara mereka berfikir, merasa dan bertindak terhadap isu-isu keselamatan yang memerlukan pemahaman yang mendalam terhadap tingkah-laku keselamatan. Melalui pendekatan penerokaan berjujukan kaedah bercampur, berdasarkan kanta teori kognitif sosial, teori budaya organisasi Wallach serta pengurusan kawalan keselamatan dari teori pencegahan lanjutan, kajian ini membangunkan model dan mengesahkan aspek-aspek sosio-organisasi tingkah laku keselamatan. Terdapat 396 data berguna yang dikumpul dari hasil soal-selidik ini. SPSS 20 dan perisian PLS-SEM telah digunakan untuk analisis faktor penerokaan dan deskriptif masing-masing. Hasil kajian soal-selidik menunjukkan bahawa pengurusan kawalan keselamatan, nilai-nilai peribadi dan tingkah laku peribadi adalah faktor ke arah pembentukan tingkah laku keselamatan yang baik. Kajian ini kemudiannya dilanjutkan ke satu kajian kes dengan menggunakan model yang dibentuk di sebuah jabatan teknologi maklumat di universiti awam. Kaji selidik itu memperolehi 90 data. Kajian kes ini mendedahkan bahawa budaya keselamatan organisasi, nilai-nilai peribadi serta tingkah laku mempunyai pengaruh yang signifikan ke arah tingkah laku keselamatan maklumat. Temu bual sorotan bersama tiga orang pekerja atasan di jabatan berkenaan menyokong dapatan kuantitatif kajian kes. Maka dapatlah disimpulkan bahawa nilai-nilai peribadi dan elemen-elemen tingkah laku adalah faktor paling penting yang mempengaruhi tingkah-laku keselamatan maklumat pekerja-pekerja yang bekerja dalam persekitaran awan SaaS. Walau bagaimanapun, budaya organisasi dan pengurusan kawalan keselamatan adalah faktor-faktor yang berasaskan konteks kajian kerana faktor-faktor ini bergantung kepada bagaimana organisasi dikendalikan oleh pengurusan tertinggi masing-masing. Kajian ini menyumbang kepada pengetahuan di bidang sistem maklumat melalui pembangunan model integrasi tingkah laku keselamatan yang disahkan melalui kaji selidik dan kajian kes dan saranan gagasan-gagasan baru. Hasilnya membantu penyelidik untuk lebih memahami tingkah laku keselamatan dalam konteks persekitaran perkomputeran awan SaaS di Malaysia amnya dan di jabatan yang dikaji khasnya. Model yang dibangunkan dan gagasan-gagasan baru yang diutarakan dalam penyelidikan ini dapat membantu penyelidik lain untuk memulakan kajian yang berkaitan pada masa hadapan.

ACKNOWLEDGEMENTS

Alhamdulillah, my greatest gratitude to Allah the almighty. With His blessings, I finally accomplished this journey. Lahawla wala quwata illa billahil aliyil azim.

I would like to express my high appreciation to my fatherly main supervisor, Prof Dr Mokhtar Mohd Yusof, for his wisdom, knowledge and patience in guiding me throughout my PhD journey. Thank you also to my co-supervisor, Dr Zeratul Izzah Mohd Yusoh for giving her support and advices in making sure that this journey is ended successfully. May Allah bless both of you with the best rewards for your good deeds.

My utmost gratitude also goes to my husband Dr Nuradli Ridzwan Shah Mohd Dali, my mother Hajjah Fatimah Ma'mur, my father Haji Abdul Hamid Abdul Majid, and all my children Nur Fatini Humaira, Nur Dalili Fahimah, Muhammad Lokman Mukri Shah, Luqman Al-Hakim Shah and Nur Iman Amanina, for their love, never-ending support and prayers. I could not have done it without them!

Many thanks to USIM, UTeM and Ministry of Higher Education, for giving me the opportunity to pursue my postgraduate studies. I would like to thank my proof readers Ms Azila Komar and Dr Nuradli Ridzwan Shah for their job well done. Many thanks as well to the appointed external and internal examiners for their constructive comments and advices. Lastly, to all of you who are not addressed in here but were directly or indirectly involved in this journey, your presence and assistance are highly appreciated.

Jazakallah khayran khatira.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

ACCA	-	Asian Cloud Computing Association
ARPANET	-	Advanced Research Projects Agency Network
AVE	-	Average Variance Extracted
BHV	-	Behaviour
BRCTC	-	Bureaucratic
CB-SEM	-	Covariance Based Structured Equation Modelling
CCTV	-	Closed-circuit Television
CIA	-	Confidentiality Integrity Availability
COBIT	-	Control Objectives for Information and Related Technologies
COCO	-	Confidential Consortium
DT	-	Deterrence Theory
EDT	-	Extended Deterrence Theory
EFA	-	Exploratory Factor Analysis
ENV	-	Environment
GSA	-	General Service Administration
HHS	-	Department of Health and Human Services
IaaS	-	Infrastructure as a Service
INVTV	-	Innovative
IoT	-	Internet of Things

IPCA	-	Information Protection Culture Assessment
IS	-	Information System
ISC	-	Information Security Culture
ISB	-	Information Security Behaviour
ISO	-	International Organisation for Standardisation
IT	-	Information Technology
ITIF	-	Information Technology and Innovation Foundation
IQR	-	Inter Quartile Range
KMO	-	Kaiser-Meyer-Olkin
MAMPU	-	Malaysian Administrative Modernization and Planning Unit
MDeC	-	Malaysian Digital Economy Corporation
MMCI	-	MSC Malaysia Cloud Initiative
MSC	-	Multimedia Super Corridor
MyCERT	-	Malaysian Certified Emergency Response Team
NASA	-	National Aeronautics and Space Administration
NGO	-	Non-governmental Organisation
NIST	-	National Institute of Science and Technology
OC	-	Organisation Culture
PaaS	-	Platform as a Service
PLS-SEM	-	Partial Least Square Structured Equation Modelling
PMT	-	Protection Motivation Theory
PRCTC	-	Practice
PSM	-	Physical Security Monitoring
PV	-	Personal Values
RAM	-	Risk Analysis and Management

RFID	-	Radio-Frequency Identification
SaaS	-	Software as a Service
SCM	-	Security Control Management
SCT	-	Social Cognitive Theory
SESE	-	Skills Experience and Self-Efficacy
SETA	-	Security Education Training and Awareness
SME	-	Small and Medium Enterprise
SNS	-	Social Network Service
SPP	-	Security Policies and Procedures
SPRTV	-	Supportive
SPSS	-	Statistical Package for the Social Sciences
SSO	-	Single Sign On
TPB	-	Theory of Planned Behaviour
TRA	-	Theory of Reasoned Action
VM	-	Virtual Machine
WOC	-	Wallach Organisation Culture
WOCI	-	Wallach Organisation Culture Index

LIST OF PUBLICATIONS

Abdul-Hamid, H., Yusof, M.M., Mohd Dali, N.R.S. 2017. Security Compliance Behaviour of SaaS Cloud Users: A Pilot Study. *Journal of Engineering and Applied Sciences*, 15(15), pp. 4150-4155.

Abdul Hamid, H., Yusof, M. M. 2016. Conceptualizing Global Cloud Landscape: A Review of Adoption Issues and Challenges. *Research Journal of Applied Sciences*, *11*(6), pp. 333–339.

Abdul Hamid, H., Mohd Yusof, M. 2015. State-of-the-Art of Cloud Computing Adoption in Malaysia: A Review. *Jurnal Teknologi (Sciences and Engineering)*, 77(18), pp. 1–6.

CHAPTER 1

INTRODUCTION

1.1 Introduction

This study focuses on the information security behaviour assessment (ISB) of employees in the context of Software-as-a-Service (SaaS) cloud computing environment.

Organisations in the whole world have been adopting computer-based information systems (IS) to gain business values ever since its introduction in the early 1960s. The strategic IS play a vital role in aligning the business goals of the organisation with the advent of information technology (IT) to achieve its business values as well as to gain competitive advantage. Nevertheless, the rapid development of information technology has revolutionised IS and changed the way business is done in the organisations.

In the current situation, with the advent technology of Internet of Thing (IoT), a more sophisticated technology called cloud computing has emerged to transform the business landscape globally. Whilst cloud computing offers significant advantages to the adopters and users, it also comes with challenges. There is no secret that security has become the main concern and barrier that deter many organisations from adopting cloud computing (Dua, 2014).

Gartner, a renowned IT consulting, highlighted that security, environment and governance are still the main factors affecting cloud adoption (Gartner, 2015) and this notion is in line with the challenges reported by NIST (Mell and Grance, 2009). Bachlechner et al. (2014) confirmed that cloud computing faces challenges in terms of auditing clouds, managing heterogeneity of services, coordinating involved parties, managing relationship between clients and vendors, localising and migrating data and more importantly, coping with the lack of security awareness.

For instance, security incidents have happened recently which prove this claim. In January 2015, the website of Malaysian Airlines, a government linked company, was hacked by Lizard Squad; an image of a lizard wearing a hat with the caption of "Plane-Not-Found," was displayed on the website, following the incident of the missing MH370 in 2014. Prior to that, Lizard Squad attacked Sony Play station and Microsoft Xbox Live. Google Malaysia was also hacked and this happened in April 2015 where users were redirected to the hacker site claimed as Bangladeshi Tigermate hacker (Hamzah, 2015). All these incidents negatively influence the decision makers in adopting cloud computing in the organisations. Analysis done in April 2015 by Malaysian Computer Emergency Response Team (MyCERT), a security agency of Cyber security Malaysia, reveals that security incidents happen all the time with spam being the highest vulnerability, followed by fraud, intrusion, cyber harassment, malicious code, intrusion attempt and denial of service.

Computer scientists have come up with various technical solutions to overcome security hindrance. Yet, security incidents still occur over time. Information security in cloud is much challenging than in the traditional IS because cloud is a shared computing environment. Security threats are everywhere, and the risks are higher in the cloud environment. Technical solutions alone are not sufficient to protect the information in cloud environment. Therefore, inculcating ISB as part of the whole security solutions of cloud computing may help boost the level of cloud adoption.

1.2 Statement of the Purpose

This research mainly aims at assessing the information security behaviour of employees in the SaaS cloud environment.

1.3 Research Background

Due to the emerging phenomenon of cloud computing, the researcher has been putting a great deal of interest to investigate the adoption and utilisation of cloud computing among users. Cloud computing is known to have the flexibility of offering the latest dynamic IT services with lower associated costs as asserted by Al-Badi et al.(2017). However, despite its tremendous advantages, it was found that the adoption growth is much slower than anticipated due to security obstacle (Zhang et al., 2017).

Security has become and is nevertheless the major issues of information technology adoption inclusive cloud computing (Rebollo et al., 2015) . The exposure to security threats is more critical and the risks are greater in cloud environment. Various security technical protections have been employed to protect information systems in cloud from risks, threats and vulnerabilities such as cryptography, biometric and firewalls within and beyond the four walls of the organisations. However, security breaches still happen and keep rising over time.

Of all the causes, human is the main vulnerability (Miller et al., 2015) and is the weakest link of security breaches (AlHogail, 2015) inside or outside of the organisation, since any human errors, intentionally or accidentally, can compromise the security protection. The people's characteristics, shared values and norms shape their security behaviour in cloud computing environment thus affecting the safety of the information. A security breaches study reported that the employees and former staff are the main culprits of security incidents, however, current and