DETERMINING CRITICAL SUCCESS FACTORS OF INFORMATION SECURITY KNOWLEDGE TOWARDS ORGANISATIONS' INFORMATION SECURITY EFFECTIVENESS

ROHANA BINTI MOHAMAD RASHID

Thesis submitted to the Centre for Graduate Studies, Universiti Pertahanan Nasional Malaysia, in fulfilment of the requirements for the Degree of Doctor of Philosophy (Computer Science)

September 2020

ABSTRACT

It is very difficult to achieve information security effectiveness in an organisation when the biggest problem stems from people factor. The lack of awareness and understanding of information security knowledge (ISK) coupled with the lack of security awareness on security behaviour amongst employees; are the top contributing factors towards internal security incidents. No matter how great the technology, which is applied in the organisation, if the employees still retain their non-secure behaviour in the organisation, not only it will jeopardise their own self but the whole organisation as well. Therefore, it is important to continuously educate people in the organisation in managing these types of incidents and guide them towards appropriate behaviour and practice in their daily work routines.

This thesis seeks to investigate the critical success factors of ISK in Malaysian public sector organisation (MPSO). Through systematic literature review (SLR), this thesis proposes five critical success factors of ISK that affect the organisations' information security effectiveness. These critical success factors are knowledge, employee behaviour, knowledge sharing, motivation, and protection of information. In addition, through SLR, this thesis highlights the role of leadership as a moderating factor amongst the critical success factors of ISK and organisations' information security effectiveness. Self-administered questionnaire is employed to collect data from Information and Communication Technology (ICT) division in several organisations in the Malaysian public sector.

The research model is then developed and tested using partial least square (PLS) technique. SPSS 22 and SMART PLS 2.0M3 are used to validate the research model and test the proposed research hypotheses.

Based on the findings, the organisations' information security effectiveness was influenced positively by knowledge (β=0.092, t=2.028, p<0.05), employee behaviour (β=0.091, t=1.734, p<0.1), motivation (β=0.108, t=2.261, p<0.05) and protection of information (β = -0.119, t = 2.283, p < 0.05). However, knowledge sharing did not positively impact the organisations' information security effectiveness (β = 0.001, t = 0.023, p<0.1). It was also found that leadership moderated the relationship between employee behaviour and organisations' information security effectiveness (β=0.167, t=1.904, p<0.1), knowledge sharing and organisations' information security effectiveness (β=0.146, t=2.390, p<0.05), motivation and organisations' information security effectiveness (β=0.163, t=4.993, p<0.01), and lastly protection of information and organisations' information security effectiveness (β=0.123, t=3.259, p<0.01). However, the finding showed that leadership did not moderate the relationship between knowledge and organisations' information security effectiveness (β= 0.151, t=1.110, p<0.1). This research provides a conceptual model of ISK which is the main contribution of this research that can be a used as a guideline to MPSO operations (includes security practices) towards achieving organisations' information security effectiveness.

ABSTRAK

Adalah sangat sukar untuk mencapai keberkesanan keselamatan maklumat apabila masalah yang terbesar datangnya dari faktor manusia. Kurangnya kesedaran dan kefahaman tentang pengetahuan keselamatan maklumat (ISK), dan kurangnya kesedaran keselamatan mengenai tingkah laku keselamatan di kalangan pekerja adalah faktor yang paling menyumbang kepada insiden keselamatan dalaman. Tidak kiralah betapa hebatnya teknologi yang diterapkan di dalam organisasi, sekiranya perkerja masih mengekalkan tingkah laku yang tidak selamat dalam organisasi, bukan sahaja akan membahayakan diri mereka sendiri tetapi juga kepada organisasi. Oleh itu, adalah penting untuk terus mendidik orang di dalam organisasi dalam menguruskan jenis insiden ini dan membimbing mereka ke arah tingkah laku dan amalan yang sesuai dalam rutin kerja harian mereka.

Tesis ini bertujuan untuk mengkaji faktor kejayaan penting ISK dalam organisasi sektor awam Malaysia (MPSO). Melalui tinjauan literatur sistematik (SLR), penulis telah mencadangkan lima faktor kejayaan penting ISK yang mempengaruhi keberkesanan keselamatan maklumat organisasi, iaitu pengetahuan, tingkah laku pekerja, perkongsian pengetahuan, motivasi, dan perlindungan maklumat. Melalui SLR, penulis mencadangkan peranan kepemimpinan sebagai faktor penyederhanaan antara faktor kejayaan kritikal keberkesanan keselamatan maklumat ISK dan organisasi. Soal selidik yang dikendalikan sendiri digunakan untuk mengumpulkan data dari bahagian ICT di sektor awam Malaysia. Model kajian kemudian diuji menggunakan teknik *partial*

least square (PLS). SPSS 22 dan SMART PLS 2.0M3 digunakan untuk mengesahkan model kajian dan menguji hipotesis penyelidikan yang dicadangkan.

Berdasarkan hasil penemuan penyelidikan, keberkesanan keselamatan maklumat organisasi dipengaruhi secara positif oleh pengetahuan (β=0.092, t=2.028, p<0.05), tingkah laku pekerja (β=0.091, t=1.734, p<0.1) , motivasi (β=0.108, t=2.261, p<0.05), dan perlindungan maklumat (β = -0.119, t =2.283, p< 0.05) . Hasil penemuan penyelidikan juga menunjukkan bahawa perkongsian pengetahuan tidak memberi kesan positif kepada keberkesanan keselamatan maklumat organisasi (β = 0.001, t = 0.023, p<0.1). Hasil penemuan juga menunjukkan bahawa kepimpinan mempunyai hubungan moderasi antara tingkah laku pekerja dan keberkesanan keselamatan maklumat organisasi (β=0.167, t=1.904, p<0.1), perkongsian pengetahuan dan keberkesanan keselamatan maklumat organisasi (β=0.146, t=2.390, p<0.05), motivasi dan keberkesanan keselamatan maklumat organisasi (β=0.163, t=4.993, p<0.01) dan perlindungan keselamatan dan keberkesanan keselamatan maklumat organisasi (β=0.123, t=3.259, p<0.01). Walaubagaimanapun, hasil penemuan menunjukkan bahawa kepimpinan tidak mempunyai hubungan moderasi antara pengetahuan dan keberkesanan keselamatan maklumat organisasi (β= 0.151, t=1.110, p<0.1). Kajian ini akan membangunkan model teori ISK yang merupakan sumbangan utama kajian yang dapat menjadi garis panduan kepada MPSO semasa melakukan sebarang kerja (termasuk amalan keselamatan) ke arah keberkesanan keselamatan maklumat organisasi.

ACKNOWLEDGEMENTS

In the Name of Allah, the Most Gracious, the Most Merciful and, peace and blessings be upon Prophet Muhammad (S.A.W). ALHAMDULILLAH, all praise is due to Allah, The Almighty, for giving me this precious opportunity to complete my PhD thesis.

I would like to extend my heartfelt gratitude to my supervisor, Professor Ts. Dr. Omar Bin Zakaria for his patience, never-ending encouragement, precious supervision, supportive advice, and constructive suggestions for the duration of my research up to the completion of my thesis. Thank you very much for everything Prof. Only Allah SWT can repay all your kindness, and may Allah bless you and your family.

I also would like to express a very special appreciation to my dearest husband, Mohd Nabil bin Zulhemay, who is the one responsible for encouraging me to pursue the PhD. Thank you so much for being by my side from day one until the completion of this research. Thank you for your understanding, motivation, and endless support.

Last but not least, to my mother, my late father, my siblings, and my in-laws; who always motivate and support me in my studies. Thank you!

To my husband, my mother and my family

APPROVAL

The Examination Committee has met on 22nd January 2020 to conduct the final examination of Rohana Binti Mohamad Rashid on her degree thesis entitled 'Determining Critical Success Factors of Information Security Knowledge towards Organisations' Information Security Effectiveness'. The committee recommends that the student be awarded the Doctor of Philosophy (Computer Science).

Members of the Examination Committee were as follows.

Prof. Dr. Hjh Fatimah Binti Dato Ahmad
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Chairman)

Prof Madya Dr. Mohd Nazri bin Ismail
Faculty of Defence Science and Technology
Universiti Pertahanan Nasional Malaysia
(Internal Examiner)

Prof. Ts. Dr. Rabiah Binti Ahmad
Faculty on Information and Communication Technology
Universiti Teknikal Malaysia Melaka
(External Examiner)

Prof. Madya Dr. Mohd Zalisham Bin Jali
Faculty on Science and Technology
Universiti Sains Islam Malaysia
(External Examiner)

APPROVAL

This thesis was submitted to the Senate of Universiti Pertahanan Nasional Malaysia and has been accepted as fulfilment of the requirements for the degree of **Doctor of Philosophy (Computer Science)**. The members of the Supervisory Committee were as follows.

Prof. Ts. Dr. Omar Bin Zakaria

Faculty of Defence Science and Technology

Universiti Pertahanan Nasional Malaysia

(Main Supervisor)

UNIVERSITI PERTAHANAN NASIONAL MALAYSIA

DECLARATION OF THESIS

Student's full name : **ROHANA BINTI MOHAMAD RASHID**

Date of birth : **1st OCTOBER 1986**

Title : **DETERMINING CRITICAL SUCCESS FACTORS OF INFORMATION SECURITY KNOWLEDGE TOWARDS ORGANISATIONS' INFORMATION SECURITY EFFECTIVENESS**

Academic session : **2019/2020**

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

I further declare that this thesis is classified as:

☐ **CONFIDENTIAL** (Contains confidential information under the official Secret Act 1972)*

☐ **RESTRICTED** (Contains restricted information as specified by the organisation where research was done)*

☐ **OPEN ACCESS** I agree that my thesis to be published as online open access (full text)

I acknowledge that Universiti Pertahanan Nasional Malaysia reserves the right as follows.

1. The thesis is the property of Universiti Pertahanan Nasional Malaysia.
2. The library of Universiti Pertahanan Nasional Malaysia has the right to make copies for the purpose of research only.
3. The library has the right to make copies of the thesis for academic exchange.

Signature of student	Signature of main supervisor
861001-35-5052	**OMAR BIN ZAKARIA**
IC/Passport No. of student	Name of supervisor
Date: 27 August 2020	Date: 27 August 2020

Note: *If the thesis is CONFIDENTAL OR RESTRICTED, please attach the letter from the organisation stating the period and reasons for confidentiality and restriction.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AVE	Average Variance Extracted
CFA	Confirmatory Factor Analysis
CR	Composite Reliability
CSF	Critical Success Factors
DIKW	Data, Information, Knowledge, Wisdom
EB	Employee Behaviour
ICT	Information Communication and Technology
IS	Information Security
ISK	Information Security Knowledge
IT	Information Technology
KM	Knowledge Management
KN	Knowledge
KS	Knowledge Sharing
LDR	Leadership
MIS	Management Information System
MPSO	Malaysian Public Sector Organisation
MT	Motivation
OISE	Organisations' Information Security Effectiveness
POI	Protection of Information
SETA	Security Education Training Awareness

CHAPTER 1

RESEARCH ORIENTATION

1.1 Introduction

Knowledge is considered as the main key for competitiveness amongst organisations and also one of the most important production resources which enables organisations to generate profit (Glaser & Pallas, 2007). People need knowledge to choose better solutions so that good decisions can be made, and the right and most appropriate actions can be taken. In the context of information security, having adequate knowledge on information security at all levels in the organisation, provides lots of advantages to the organisation. People with the knowledge on information security would know how to protect the organisation's assets from being accessed by unauthorised person. Information security generally covers the protection of information and its

critical elements, including systems and hardware that use, store and transmit that information (Whitman & Mattord, 2012).

IT Governance Institute (2006) proposed that in order to achieve effectiveness in today's complex interconnected world, information security must be addressed at the highest level by the organisation. The rapid growth of technology has forced many organisations to deal with enormous technological device in order to ensure that they keep abreast of the current technology. Nowadays, many organisations depend on information system (IS) and information technology (IT) in running their businesses therefore, the protection of information assets becomes an important and serious issue. As more organisations get connected and invest into IT, the security concerns will ultimately grow and new threats will emerge, thus making the organisations vulnerable. In order to maintain information security in an organisation, the commitment of employees at all levels is required. The lack of commitment and support from all employees in being involved in information security work may jeopardise the security mechanism (Albrechtsen, 2007; Hagen & Albrechtsen, 2009).

Insufficient attention to human factors in system design and implementation for Information Communication Technology (ICT) outsourcing project contribute to most of information security issues that probably influence other security risk factors (Albrechtsen, 2007; Khidzir, Mohamed, & Arshad, 2010). Therefore, the lack of information security knowledge may lead to the ineffectiveness of organisation in handling security problems such as loss of valuable data and information, leakage of

confidential data, data theft and so on (Siu & Hui, 2011; D. W. Straub & Welke, 1998). Thus, the drive for an effective information security should come from top management. If the top management apply their knowledge in their work and encourage the employees to similarly do so in their daily work, the effectiveness of information security in organisation can be achieved and at the same time, minimise internal security incidents (Mittal, Roy, & Saxena, 2010).

1.2 Problem Statement

In this globalisation era, technology is evolving rapidly, and business must keep abreast of this evolution to remain competitive in today's business world. This emerging IT trend could impact the organisations' information security effectiveness. Statistics from Malaysia Computer Emergency Response Team (MyCERT) showed that, from nine incidents reported to Cyber Security Malaysia from year 2012 to 2019, fraud continues to be the biggest incident reported over the years. Although from 2014 to 2015, there was a decrease in the number of cases reported, but from 2016 to 2019 the cases reported showed a continuous increase (see Table 1.1 and Figure 1.1).

Table 1. 1: Percentage of Reported Incidents Based on General Incident Classification Statistics 2012-2019

Incident Classification	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**
Fraud	40.00	42.17	37.57	32.85	47.05	47.99	47.88	72.17
Cyber Harassment	3.00	4.81	4.63	4.46	6.35	7.03	3.33	2.41
Spam	5.27	8.93	30.63	35.69	6.54	4.32	3.20	1.20
Intrusion	43.36	26.04	9.44	17.29	29.71	25.26	10.84	12.62
Denial of Service	0.23	0.18	0.24	0.38	0.79	0.50	0.09	0.18
Content Related	0.20	0.51	0.29	0.33	0.60	0.58	1.04	2.77
Intrusion Attempt	0.67	0.71	10.92	3.06	3.32	3.34	16.87	0.97
Malicious Code	6.47	16.46	6.01	5.72	5.22	10.22	15.89	6.85
Vulnerabilities Report	0.78	0.18	0.29	0.22	0.42	0.75	0.86	0.84
Total Cases Reported	9967	10636	11918	9915	8334	7962	10699	10772

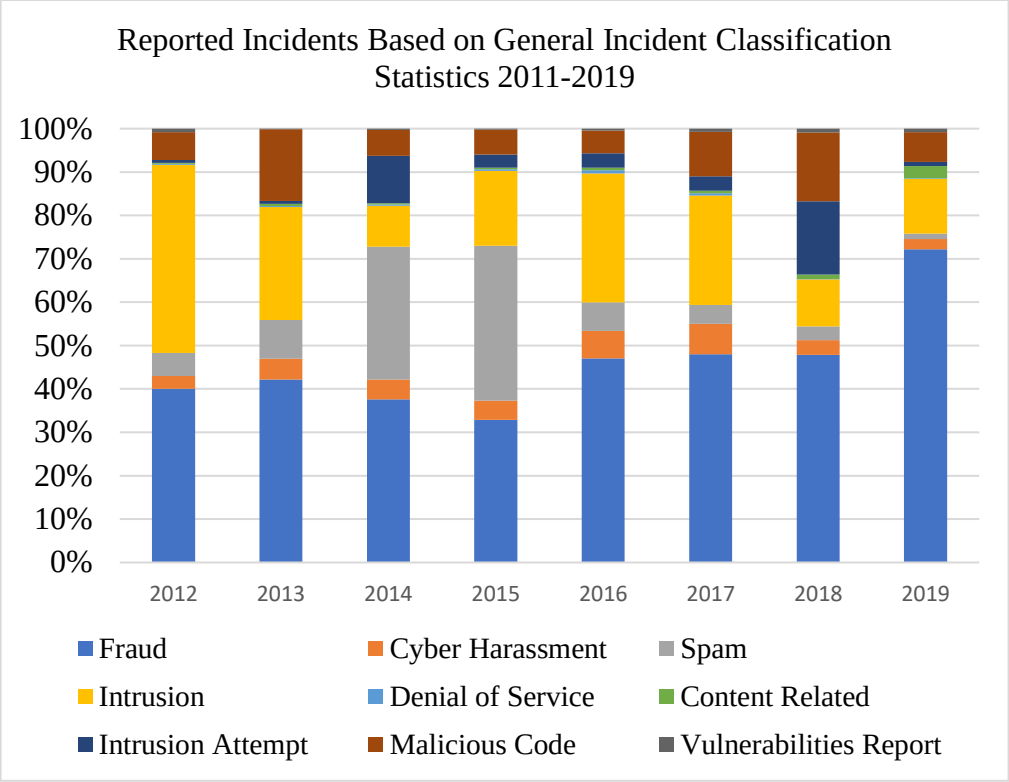

Figure 1. 1: Reported Incidents Based on General Incident Classification Statistics 2011-2019

This indicates that more people in organisations are becoming victims to online fraud which includes phishing emails such as business emails compromise and malware (Raj, 2020). While cyber security measures have been taken by many organisations, the percentage of cases reported such as fraud is still on the increase. In Malaysian public sector organisations, employees are advised to avoid websites that are not related to their work (Raj, 2020). However, the use of personal mobile devices such as hand phones, tabs or personal laptops through the organisation's Wi-Fi to access the internet by some of employees can lead to cyber security issues such as malware; that can go through their devices onto the organisation's network and may lead to the access of unauthorised company information as their devices are not protected (Raj, 2020). Therefore, it is

important that the organisation's information and the dissemination of information should be restricted so that it can be controlled more effectively. It is often said that the weakest link in an organisation is the people inside the organisation itself (Furnell & Clarke, 2012; Metalidou et al., 2014; Safa & Maple, 2016). This seems particularly true looking at the number of reported cases above. No matter how great the technology is applied in the organisation, if the employees do not take these issues seriously and still retain their non-secure behaviour in the organisation, not only will jeopardise their own self but the organisation as well. Therefore, it is important to continuously educate people in the organisation in managing these types of incidents and guide them towards appropriate behaviour and practice in their daily work routines.

Next in the list is intrusions which contribute to the second largest incidents besides fraud from 2012 to 2019. Even though the percentage of cases reported on intrusion showed a slight decrease in 2018, but in 2019 the number of intrusion cases reported keeps increasing. This is where organisations need to ensure that they apply cyber security protection that is up to date and has all the latest patches. Kassim and Abdullah (2017) stressed that system administration needs to apply security patches, keep servers or application up to date with current patches and follow best practices for web application so as to keep attackers away.

Although many proactive measures and appropriate approaches to assess the level of risk of ICT assets have been undertaken, the problem of internal security incidents is still at an alarming level (see Figure 1.1) and this will surely affect the organisations'

information security effectiveness. It is well known that cyber security is technologically related. Technology is obviously a major part of cyber security, but technology alone is not enough to protect organisations from threats. An effective cyber security requires people, process, and technology in managing an organisation's business operation (Posthumus & von Solms, 2004). The concept of combining people, process, and technology in information security is nothing new. This concept shows that these three factors are interdependent because people are the ones who implement the process and use the technology as tools. The misuse or abuse of one or all factors will affect the whole organisation. The right security control which should comprise of people, process and technology, has to be in place to prepare, protect, and respond to all types of internal or external cyber threats. Organisation may have the technology, but without proper processes and well-trained employees (people), would result in vulnerabilities which could harm the whole organisation. As stated by Bonderud (2016), organisation should invest in people together with the technology to make full sense of security technology in the organisation. When it comes to protecting the organisation's assets against insider threats, how the people and process are set up to mitigate the risk from employees' behaviour which creates an opportunity for threats to occur in the workplace; is too often overlooked. This include the failure to follow policies, guidelines and procedures set by the organisation.

In addition, the lack of information security knowledge on the roles and responsibilities in information security is one of the 'people' problems prevalent in an organisation which would lead to internal security incidents. Usually, the job descriptions