INFORMATION SECURITY BEHAVIOR IN ORGANIZATIONS: INFLUENCING FACTORS AND MANAGEMENT STRATEGIES

BY

OMAR BARZAK

A thesis submitted in fulfilment of the requirement for the degree of Doctor of Philosophy in Information Technology

Kulliyyah of Information and Communication Technology
International Islamic University Malaysia

DECEMBER 2020

ABSTRACT

Employees security behavior is a challenge to the confidentiality, integrity, and availability (CIA) of organizational information. This is because there have been cases of employees compromising organizational information systems (IS) through their behavior whether it is performed with or without intention. Although information security studies are now focusing on insiders' security behaviors and their impacts on IS, they do not effectively differentiate between security behavior that is intentional or unintentional, and compliant or non-compliant to information security policies. While many studies focus on controlling and preventing unacceptable security behavior, studies that focus on factors encouraging good and desired security behavior are limited. Hence, this research aims are twofold: firstly, to identify different types of intentional and unintentional information security behavior, for both compliant and non-compliant, and; secondly, to examine their influencing factors in order to suggest a taxonomy of information security behavior. By understanding the different categories and influencing factors of employee's security behavior, organizations may be able to address such behavior in order to protect organizational IS. Security literature has shown that organizations can reduce information security incidents and the cost of technical countermeasures by managing their employees' security behavior. A recent report from security industry reveals that organizations in the Middle East are being targeted by cyber attackers due to the wealth of the countries and information security practices that are below par in the region. Additionally, security studies suggest examining employees' security behavior in different cultures and regions, as the majority of the previous studies were conducted in Western culture. Conceptual security behavioral model is proposed based on contemporary information security studies inspired by Islamic principles. Following this, qualitative research approach and multiple-case study on four organizations in Gulf Countries was conducted by interviewing both employees and managers. Moreover, document reviews and participant observation were applied to validate feedback from the participants. The findings indicated that employees' security culture played an essential role in information security behavioral compliance. Although employees showed their interest to comply with information security policies, non-compliant security behavior was still prevalent since they were lacking in security literacy and awareness. Furthermore, the case organizations' security countermeasures need to be improved by developing, implementing and enforcing information security policies which are clearly communicated to and understood by all employees. Similarly, the organizations too, need to understand their employees' behavior. The research findings are corroborated into a proposed model called Integrated Security Behavioral Model (ISBM). ISBM may benefit organizations since the model can be used in assessing, planning and managing their employees' security behavior and improve their security strategies. The thesis contributes to both research and practice; by fulfilling the research gaps stated above and improve organizations' best practices through the understanding of employees' different types of security behavior.

خلاصة البحث

إن التحديات التي تواجه توفُّر وسريَّة وسلامة محتوى المعلومات قد أصبحت كبيرة بسبب سلوك الموظفين تجاهها؛ يعود ذلك للحوادث المتكرِّرة للموظَّفين الذين أضرُّوا بسلامة أمن المعلومات، بسبب سلوكهم المقصود أو غير المقصود تجاه أمن المعلومات. ورغم أنَّ الدراسات الحاليَّة تركِّز على سلوك الموظَّفين تجاه أمن المعلومات وتأثيرهم على أنظمة المعلومات، إلا أن هذه الدراسات لم تفرِّق بشكلٍ فعَّالٍ بين سلوك الموظَّفين المتسبِّب بحوادث أمن المعلومات بشكلٍ مقصودٍ أو غير مقصود، وبين السُّلوك الملتزم وغير الملتزم أيضاً. هناك دراساتٌ أخرى كثيرة قد ركَّزت على منع السُّلوك غير المرغوب به تجاه أمن المعلومات، في المقابل فإنَّ الدراسات التي ركَّزت على سلوك الموظفين الإيجابي تجاه أمن المعلومات وتشجيعه كانتْ محدودة. لذلك كان لهذا البحث هدفان رئيسيَّان: الأول: يكمن في تحديد الأنماط المختلفة لسلوك الموظَّفين تجاه أمن المعلومات بجانبيهما الملتزم وغير الملتزم. والثاني: تحديد الدَّوافع وراء سلوك الموظَّفين الأمني تجاه أمن المعلومات وتصنيف كل سلوكٍ على حِدَه، حيث إنَّ فهم أنماط سلوك الموظفين المختلفة تجاه أمن المعلومات سَيسهِّل للشَّركات تحديدَ الحلول لأنماط السُّلوك المختلفة، والتي ستؤهِّلها لحماية قواعد معلوماتها. في الواقع، فإنَّ الدراسات الأمنية أثبتتْ أنَّ الشَّركات بإمكانها تقليل حوادث أمن المعلومات والتكاليف الباهظة التي تُدفع على التَّدابير التَّقنية من أجهزة ومعدَّات وبرامج، وذلك بإدارة سلوك الموظَّفين الأمني تجاه المعلومات. الدِّراساتُ شجَّعت أيضاً على أنْ تكون هناك دراساتٌ لسلوك الموظَّفين تجاه أمن المعلومات في ثقافاتٍ متعدِّدة، ومناطق مختلفة حيث أنَّ معظم الدراسات السابقة تمَّت في الدول الغربية وثقافتها. تم اقتراح نموذج السلوكيات الأمنية بناء على النظريات الغربية وذلك بدمجها مع المفاهيم والمبادئ الإسلامية. دراسة الحالة المتعدِّدة تمَّت في أربعِ شركاتٍ في دول الخليج العربي وذلك من خلال إجراء مقابلاتٍ مع الموظَّفين والمدراء. كما تم أيضا مراجعة الوثائق المتعلقة بأمن المعلومات والمراقبة لسلوك الموظفين الأمني لتأكيد المعلومات التي تم جمعها من الموظفين والمدراء. نتائج البحث توصَّلت بأنَّ ثقافة أمن المعلومات لدى الموظفين تقوم بدورٍ أساسيٍّ في التزام الموظفين تجاهها. ورغم أنَّ الموظفين أظهروا اهتماماً في الالتزام بضوابط أمن المعلومات، إلا أنَّ عدم الانضباط كان هو السَّائد، ويرجع ذلك لضعف المعرفة بأمن المعلومات وقلَّة التوعية من جهة أخرى. وبالإضافة إليه فإنَّه يجب تحسين التَّدابير الأمنيَّة لأمن معلومات المنظَّمات من خلال تطوير ووضع سياسات أمن المعلومات. هذه السِّياسات والضَّوابط يجب أن تبلَّغ للموظَّفين بشكلٍ واضحٍ وبدون مُلابسات، وعلى الشَّركات التَّأكُّد من أنَّ الموظفين قد استوعبوا تلك السِّياسات والضَّوابط. وفي ذات الوقت، فإنَّ على الشركات فهم سلوك موظفيها تجاه أمن المعلومات .نتائج البحث تمَّ عرضها من خلال نموذجٍ يعرضُ سلوكيَّات الأمن المتكاملة (ISBM). وهو ما سيفيدُ المنظَّمات من خلال استخدام ذلك النموذج في تقييم وتخطيط وإدارة السُّلوكيات الأمنيَّة لموظَّفيها.

APPROVAL PAGE

The thesis of Omar Barzak has been approved by the following:

Nurul Nuha Abdul Molok
Supervisor of Supervisory Committee

Murni Mahmud
Chairman of Supervisory Committee

Shuhaili Talib
Member of Supervisory Committee

Abdul Rahman Ahlan
Internal Examiner

Mohd Zalisham Bin Jali
External Examiner

Atif Ahmad
External Examiner

Amir Akramin Shafie
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Omar Barzak

Signature .... Date ....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

INFORMATION SECURITY BEHAVIOR IN ORGANIZATIONS: INFLUENCING FACTORS AND MANAGEMENT STRATEGIES

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Omar Barzak

……..…………………….. …………………………..
Signature Date

This thesis is dedicated to my family, friends and other well-wishers for their support in its entire ramification toward making my dream of acquiring a Ph.D. degree a reality.

ACKNOWLEDGEMENT

All praises be to Allah, the Almighty who has given me the sustenance and patience throughout my dissertation journey.

Firstly, it is my utmost pleasure to dedicate this work to my dear parents, my brother and sisters, who granted me the gift of their unwavering belief in my ability to accomplish this goal: thank you for your support and patience.

I wish to express my deep appreciation and thanks to my supervisor, Dr. Nurul Nuha Abdul Molok for providing me with knowledge, time, guidance and encouragement during my dissertation journey.

I would like to thank the members of my supervisory committee, the chairman Dr. Murni, and my co-supervisor Dr. Shuhaili Talib for their continuous support, time, efforts and advice. Thank you for sticking with me.

Finally, special thanks to my colleagues as well as members of my extended and compound families.

Thank you all for making it possible.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

In the past decade, insiders' security behavior has captured the intention of organizations and academia (AlHogail & Mirza, 2014; Crossler et al., 2013; Fernando & Yukawa, 2013; Guo, 2013; Ifinedo, 2019b). Employees are given privileges to access organizational information systems (IS) that makes information security incidents easily occurred with or without their intentions (Aurigemma & Mattson, 2017; CERT, 2013; Colwill, 2009; Crossler et al., 2013). According to academic studies, most information security breaches are resulted from poor information security practices and human mistakes (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009; Martin & Zafar, 2015; Safa, Sookhak, et al., 2015; Warkentin & Willison, 2009). Therefore, understanding employees' security behavior and the factors affecting them can help organizations to manage their employees' security behavior and reduce security incidents (Ifinedo, 2019a; Padayachee, 2012).

In accordance to Abdul Munir, Talib, Abdul Molok, & Ahmad (2018); Crossler et al. (2013); Kreicberga (2010); Warkentin & Willison (2009), the trend of information security studies is now moving towards focusing on insiders' security behavior and their impacts on information systems (IS). In fact, insiders are the weakest link in the information security chain as they are naturally prone to make mistakes and misunderstandings (Abdul Munir et al., 2018; Crossler et al., 2013; Fernando & Yukawa, 2013; Öğütçü, Testik, & Chouseinoglou, 2016). Moreover, they are easily motivated and affected by their peers and the environment which make their actions towards IS unpredictable (Fernando & Yukawa, 2013; Hu, Xu, Dinev, & Ling, 2011).

Despite the importance of understanding information security behavior, particularly those happen without the intention of the employees to jeopardize organizational information security, academic studies that cover unintentional security threats are still limited (CERT, 2013; Crossler et al., 2013; Fernando & Yukawa, 2013; Metalidou, Marinagi, Trivellas, & Eberhagen, 2014; Safa, Solms, & Furnell, 2015; Warkentin, Straub, & Malimage, 2012). According to Abdul Molok, Ahmad, & Chang (2018); Fernando & Yukawa (2013); Liu, Wang, & Camp (2009) security incidents caused by employees are more likely to be unintentional than intentional. They also posit that most of information leakage incidents and other security breaches are resulted from accidental security behavior and human mistakes that could cause more damage to organizational IS.

In accordance to Alhogail & Mirza (2014) and Crossler et al. (2013), there are quite a number of studies about employees' security behavior. However, most of them did not attempt to differentiate between those who intentionally violate information security policies (ISP) from those unintentionally violate them. Hence, without differentiating intentional and unintentional behaviors, the effectiveness and efficiency of the procedures and recommendations to protect IS from any employees' threats could significantly be reduced (Crossler et al., 2013).

There are security studies which proposed models and frameworks that classify different kinds of employees' behavior (Jouini, Rabai, & Aissa, 2014; Leach, 2003; Loch, Carr, & Warkentin, 1992; Warkentin et al., 2012). However, a comprehensive model or framework that covers all aspects of employees' behavior such as positive and negative security behavior, and intentional and unintentional security behavior is still inadequate. Crossler et al. (2013) mentioned that information security behaviors were covered mostly in security studies that conducted in Western culture. Therefore, they urged for more information security studies in other cultures and regions. Furthermore, Gulf Countries are considered to highly suffer from cybersecurity incidents due to their financial growth and information assets along with less security practices (DarkMatter, 2019; Guven, 2018).

To fulfill the gaps stated above, this thesis explores employees' security behavior in Gulf Countries, and it is intended to achieve three aims. First, it aims to categorize employees' security behavior and provide definition for each categorized behavior. Second, it seeks to explore factors influencing employees' security behaviors. Third, it aims to investigate organizational strategies in managing employees' security behavior. Finally, based on the findings of the above aims, this thesis proposes a model that can be used by organizations to understand and address different kinds of their employees' security behaviors.

This research contributes to theoretical knowledge by assigning the Integrated Security Behavioral model (ISBM). ISBM contributes to organizational practices by allowing them to assign their security strategies by addressing different employees' security behaviors and their influencing factors. Hence, ISBM can be applied by organizations to address employees' vulnerabilities by implementing suitable security practices tailored to different types of security behavior (see 6.4). It also contributes to the body of knowledge in understanding employees' security behavior through the taxonomy of information security behaviors and drawing detailed security behaviors for both compliance and non-compliance security behaviors. Finally, it contributes to empirical evidences through multiple-case study on four organizations by having current insightful qualitative data that has been collected and analyzed which led to results and findings.

This chapter highlights the background of the study and why is it important to understand influencing factors of employees' security behavior. It presents the problem statement, significance of the study, research objectives, research questions, the scope, and definitions of terms. Finally, it briefly outlines the research design and overview of the thesis structure.

1.2 STATEMENT OF THE PROBLEM

1.2.1 Employees' Security Behavior

As mentioned above, employees are the weakest link in information security as it is their nature to make mistakes, they are often motivated and affected by their peers and the environment (Fernando & Yukawa, 2013; Guven, 2018; Hu, Xu, Dinev, & Ling, 2011). According to academic studies, the highest information security risk to the IS comes from employees who violate the organizational information security with or without intentions (Galvez, Shackman, & Guzman, 2015; Greitzer et al., 2014; Guo, Yuan, Archer, & Connelly, 2011; Hu et al., 2011; Johnston, Warkentin, Mcbride, & Carter, 2016).

Employees have more potential to cause harm to IS than the outsiders because they are already inside the organization, bypassing the physical or network perimeter, and have direct access to the IS. Additionally, employees have the knowledge about organization and available assets that outsiders know nothing or little about (Colwill, 2009). Employees can also target the organizational information and IS directly without facing the barriers that are faced by the external hackers (Aurigemma & Mattson, 2017; Colwill, 2009; Guo et al., 2011). More importantly, outsiders do not have the insiders' privileges. They need to collect information about the organization, and scan for IS vulnerabilities before performing their attacks. They also need to have special tools and spend a long time in order to breach the security perimeter and access the IS in which employees can do that with almost zero efforts and time (Colwill, 2009).

Employees may unintentionally reveal confidential information due to many reasons such as human errors, lapses, inattention and employees' ignorance (AlHogail & Mirza, 2014; Bulgurcu et al., 2010; Fernando & Yukawa, 2013; Galvez et al., 2015; Herath & Rao, 2009; Metalidou et al., 2014; Safa, Sookhak, et al., 2015). Hence, employees' security behavior can be divided into two, intentional and unintentional (Abdul Molok, Chang, & Atif, 2013; Crossler et al., 2013; Fernando & Yukawa, 2013; Kolkowska, Karlsson, & Hedström, 2017). Crossler et al. (2013) suggest that organizations need to differentiate between intentional and unintentional security behavior in order to have security strategies that may effectively combat employees' security threats. It is stated that, having a full view of different kinds of employees' security behavior can be very helpful for managers, auditors, and others with an interest to assess end-user security behavior in order to understand, observe and manage such behavior (AlHogail & Mirza, 2014; CERT, 2013; Crossler et al., 2013; Galvez et al., 2015; Ifinedo, 2014; Martin & Zafar, 2015). Thus, this thesis covers both intentional and unintentional information security behaviors and explore underlying sub-security behaviors related to them.

1.2.2 Influencing Factors of Employees' Security Behavior

According to Abdul Molok et al. (2018); Colwill (2009); Fernando & Yukawa (2013); Liu et al. (2009), security incidents caused by employees are more likely to be unintentional than intentional. They also posit that, most of information leakage incidents and other security breaches are resulted from accidental security behavior and human mistakes which has higher damaging impact on the security of organizational

IS. Therefore, this research also emphasizes on the importance of studying the factors influencing unintentional information security behavior of the employees and the organizational strategies to prevent such behavior in order to protect organizational IS. It is suggested that, having a comprehensive model about employees can effectively and appropriately address behavioral aspect of the problem (AlHogail, 2015; CERT, 2013; Crossler et al., 2013; Fernando & Yukawa, 2013; Galvez et al., 2015; Guo, 2013; Ifinedo, 2014).

1.2.3 Employees' Security Behavioral Studies

Although employees are known to be the weakest link of information security chain, academic studies that investigate influencing factors for end-users to engage in such behaviors are still limited (Colwill, 2009; Crossler et al., 2013; Guo et al., 2011; Herath & Rao, 2009; Kreicberga, 2010; Öğütçü et al., 2016; Warkentin & Willison, 2009). The current information security behavioral studies need to cover different regions and cultures as most of them were conducted in Western countries (Crossler et al., 2013). Since understanding different cultures and their effects on employees security behavior plays important role in understanding the phenomenon (Crossler et al., 2013), this thesis is exploring employees' security behaviors in Gulf Countries due to the fact that organizational information assets in the Middle East are highly targeted by cybersecurity attacks (DarkMatter, 2019).

In accordance to AlHogail & Mirza (2014); Crossler et al. (2013), there are quite a number of studies about employees' security behavior. However, most of them did not attempt to differentiate between those who violate information security policies with intention from those who violate them without the intention to do so. There are studies that could not effectively give clear definitions of the different types of employees' security behavior or they do not clearly differentiate between intentional and unintentional information security behavior (Bishop & Gates, 2008). Therefore, dealing with intentional and unintentional security behavior as one behavior can significantly reduce the effectiveness and efficiency of the procedures and recommendations to protect IS from any employees' security threats (Crossler et al., 2013).

Studies on employees' security behavior have been covered by current studies (see 2.5) but they mostly cover the behavior that is done with intention. Despite this huge coverage of intentional employees' security behavior, security studies that focus on unintentional security behavior are still limited (AlHogail & Mirza, 2014; CERT, 2013; Crossler et al., 2013; Galvez et al., 2015; Greitzer et al., 2014; Martin & Zafar, 2015).

Guo (2012) and Warkentin et al. (2012) mentioned that studies that focus on measuring employees' positive behavior that represents compliance security behavior are more than studies that measures the negative behavior that represents non-compliance security behavior. Warkentin et al. (2012) and Metalidou, Marinagi, Trivellas, & Eberhagen (2014) mentioned that these studies use security models and underlying theories that explain positive behavior, hence, a different model is needed to explain negative behavior. Thus, this thesis also covers both compliance and non-compliance information security behavior, malicious and non-malicious, and the factors influencing them.

1.3 PURPOSE OF THE STUDY

As the focus of information security threats landscape is moving towards employees' security behaviors and their impacts on IS (see 2.5), this thesis examines in detail about the different types of information security behaviors and the factors that are influencing them. It also addresses the suitable strategies to address these different factors that affect employees' security behavior in order to protect organizational information. The study also aims to study different strategies that organizations take to control and manage their employees' security behavior.

The study has chosen four organizations in Gulf countries to study employee security behavior following Crossler et al. (2013) who emphasizes that there is a need to study employees' security behavior of other cultures as most information security studies have been conducted in Western countries.

Although Warkentin & Willison (2009) state that the greatest threats to IS comes from deliberate actions of employees, this thesis concur with studies which state that security incidents caused by employees are more likely to be unintentional than intentional (Abdul Molok et al., 2018; Colwill, 2009; Fernando & Yukawa, 2013; Galvez et al., 2015; Liu et al., 2009; Loch et al., 1992). Moreover, unintentional security incidents could cause more damages to organizational IS (see 2.5.2) (Abdul Molok et al., 2018; Colwill, 2009; Fernando & Yukawa, 2013).

Based on our investigation on different types of security behavior, the factors that influence them and the strategies to manage them, this research provides a taxonomy and definitions of employees' security behavior. This taxonomy covers security behavior that is done with and without intentions, whether it is in compliant or non-compliant to security policies, and whether the behavior is malicious and non-malicious. Through this taxonomy, it is expected that organizations will be able to detect different types of employee security behaviors and provide suitable strategies to manage them.

1.4 RESEARCH OBJECTIVES

Based on the research gaps stated above, this study aims to achieve the following objectives:

1- To investigate different types of information security behavior.

2- To identify different influencing factors of employees' information security behavior that have impacts on organizational information security.

3- To examine contemporary information security studies and Islamic principles that are related to security studies that can be used to further enhance the taxonomy of information security behavior.

4- To study organizations' strategies in addressing employees' information security behavior.

5- To propose an integrated model of information security behavior that can be used by academia and organizations to understand such behavior and improve their security strategies.

1.5 RESEARCH QUESTIONS

In order to achieve the above research objectives, this research seeks to answer the following research questions:

1. Why do employees engage in intentional and unintentional information security behavior?

This research question attempts to understand factors that influence employees' security behavior that affect organizational information security with or without their intentions. Therefore, understanding these influencing factors helps organizations in assessing, studying, planning and controlling their employees' security behavior.

In order to understand the influencing security factors, we need to look for different types of information security behavior that influence these factors, thus addressing the research objectives 1 and 2.

2. How do organizations manage intentional and unintentional information security behavior of the employees?

This question attempts to explore the perspectives of organizations about the ways they deal with different kinds of employees' information security behavior that affect the security of IS. It investigates the security strategies implemented in the organizations in addressing employees' security behavior and the effect of organizations' security level on managing their employees' security behavior, addressing the research objective 5.

Research objectives 4 and 5 and the answers to both research questions 1, 2 were used to address the research objective 5 in which providing insights on employees' security behaviors and their influencing factors combined with organizational strategies in a behavioral model.

1.6 SCOPE OF THE STUDY

The study focuses on information security behavior of employees in four private business organizations in four different Gulf Countries namely, Kuwait, Saudi Arabia, Qatar and Oman. It is to uncover the similarities and differences among them in their employees' security behavior, factors influencing their security behavior and the different strategies that had been used by the case organizations to address their employees' security behavior. Moreover, this research also explores the influences of different cultures on employees' security behavior and how they are different from the Western security culture.