THE DEVELOPMENT OF INSIDER THREAT PREVENTION FRAMEWORK WITHIN ORGANIZATION

RAHIMAH BT MOHAMAD ZUWITA @ABU BAKAR

UNIVERSITI PENDIDIKAN SULTAN IDRIS

2023

THE DEVELOPMENT OF INSIDER THREAT PREVENTION FRAMEWORK WITHIN ORGANIZATION

RAHIMAH BT MOHAMAD ZUWITA @ABU BAKAR

THESIS PRESENTED TO QUALIFY FOR A DOCTOR OF PHILOSOPHY

FACULTY OF COMPUTING AND META-TECHNOLOGY
UNIVERSITI PENDIDIKAN SULTAN IDRIS

2023

UPSI/IPS-3/BO 32
Pind : 00 m/s: 1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Please tick (√)

Project Paper □
Masters by Research □
Master by Mixed Mode □
PhD ☑

INSTITUTE OF GRADUATE STUDIES

DECLARATION OF ORIGINAL WORK

This declaration is made on the ……12………..day of……December………..20…23…..

i. Student's Declaration:

I, RAHIMAH MOHAMAD ZUWITA, P20152002361, SENI, KOMPUTERAN, INDUSTRY KREATIF (PLEASE INDICATE STUDENT'S NAME, MATRIC NO. AND FACULTY) hereby declare that the work entitled THE DEVELOPMENT OF INSIDER THREAT PREVENTION FRAMEWORK WITHIN ORGANIZATION ______________ is my original work. I have not copied from any other students' work or from any other sources except where due reference or acknowledgement is made explicitly in the text, nor has any part been written for me by another person.

rahimah
____
Signature of the student

ii. Supervisor's Declaration:

I BAHBIBI BINTI RAHMATULLAH (SUPERVISOR'S NAME) hereby certifies that the work entitled THE DEVELOPMENT OF INSIDER THREAT PREVENTION FRAMEWORK WITHIN ORGANIZATION ______________ (TITLE) was prepared by the above named student, and was submitted to the Institute of Graduate Studies as a * partial/full fulfillment for the conferment of DOCTOR OF PHILOSOPHY INFORMATION SYSTEM AND MANAGEMENT (PLEASE INDICATE THE DEGREE), and the aforementioned work, to the best of my knowledge, is the said student's work.

12/12/2023
____
Date

Prof. Madya Dr. Bahbibi Rahmatullah
Pensyarah
Fakulti Komputeran dan Meta-Teknologi
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak

Signature of the Supervisor

UPSI/IPS-3/BO 31
Pind.: 01 m/s:1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
اونيۏرسيتي ڤنديديقن سلطان ادريس
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH / *INSTITUTE OF GRADUATE STUDIES*

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK *DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM*

Tajuk / *Title*: THE DEVELOPMENT OF INSIDER THREAT PREVENTION FRAMEWORK WITHIN ORGANIZATION

No. Matrik /*Matric's No.*: P20152002361

Saya / *I* : ______________________

(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris

2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.

3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.

4. Sila tandakan (√) bagi pilihan kategori di bawah */ Please tick (√) for category below:-*

□	**SULIT/*CONFIDENTIAL***	Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*
□	**TERHAD/*RESTRICTED***	Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restircted information as specified by the organization where research was done.*
/	**TIDAK TERHAD / *OPEN ACCESS***	

rahimah

(Tandatangan Pelajar/ Signature)

Prof. Madya Dr. Bahbibi Rahmatullah
Pensyarah
Fakulti Komputeran dan Meta-Teknologi
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak

Signature of the Supervisor

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Tarikh: 12/12/2023

Catatan: Jika Tesis/Disertasi ini **SULIT** @ **TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

ACKNOWLEDGEMENT

The highest gratitude to Allah the Almighty as with his blessings and permission I have, alas, being able to complete this dissertation for my Doctor of Philosophy.

I would like to take this opportunity to present my deepest gratitude to my supervisor, Dr. Bahbibi binti Rahmatullah, for her enthusiastic encouragement and outstanding guidance and also to Dr. Aisyah bt Salim for her excellent guidance in determining the success of this project.

Special thanks to companies and staffs that willing to participate and support in this research. To my beloved family, a million thanks for your understanding and encouragement to me throughout this dissertation journey. No words could more written to express this blessing. Alhamdulillah.

ABSTRACT

Issues related to insider threat in organization have been actively debated over the years. Despite the probability, they have a higher rate of success, can go undetected, and therefore pose a much greater risk than external adversaries. Due to those circumstances, a protective and preventive measure becomes a pitch demand to prevent any harm caused by malicious insiders. A framework has been developed based on a survey conducted. There are five objectives posed in this research; (1) To identify factors that trigger/motivate insiders to attack an organization’s data (2) To determine the relationship between security behaviours and the appraisal process in Protection Motivation Theory (3) To determine the degrees of relevance of these identified reflective factors to Protection Motivation Theory (4) To develop a framework based on the result synthesized from data analysis (5) To verify the applicability of the proposed framework through expert judgement. The research adopted a quantitative research approach that utilizes surveys to gather data from approximately 250 respondents. Structural Equation Modeling (SEM) analysis was employed for data analysis. The results strongly supported all hypotheses, recording the p-values ranging from 0 to 1. Furthermore, the findings underscore the significance of organizational factors in preventing insider threats within an organization. This insight is particularly valuable for academics who aim to develop theories and gather empirical evidence related to behavioral information security, especially considering the potential applicability of these findings in various organizational settings. As far as the amount of standardized path weights is concerned, reaction efficacy is by far the most important factor influencing insiders' desire to defend their companies from information security risks.

PEMBANGUNAN RANGKA PENCEGAHAN “INSIDER” DALAM ORGANISASI

ABSTRAK

Isu ancaman rangkaian ini menjadi suatu isu yang semakin hari menjadi ancaman yang sangat berbahaya dan tiada satu kaedah atau teknik yang dapat menyelesaikan semua ancaman tersebut. Maka sehubungan itu satu rangka dibangunkan untuk mengatasi masalah tersebut. Satu rangka kajian telah dibangunkan berdasarkan tinjuan yang telah dibuat. Terdapat lima objektif penyelidikan ini: (1) Untuk mengenal pasti faktor pencetus / mendorong orang dalam (penyerang) untuk menyerang data organisasi (2) Untuk menentukan hubungan antara tingkah laku keselamatan dan proses penilaian dalam Teori Motivasi Perlindungan (3) Untuk menentukan darjah perkaitan faktor reflektif yang dikenal pasti ini kepada Teori Motivasi Perlindungan (4) Untuk membangunkan rangka kerja yang dicadangkan berdasarkan hasil yang disintesis daripada analisis data (5) Untuk mengesahkan kebolehgunaan rangka kerja yang dicadangkan melalui pertimbangan pakar. Pendekatan kajian yang digunakan adalah kuantitatif yang mana kaedah tinjauan dalam mengumpul data digunakan. Sebanyak 250 respondent telah diterima dan data tersebut dianalisis menggunakan analisis Pemodelan Persamaan Struktur (SEM). Daripada dapatan kajian, kesemua hipotesis telah disokong yang mana bacaan nilai p berjulat dari 0 hingga 1. Tambahan pula, keputusan menunjukkan faktor organisasi merupakan faktor yang perlu diambil kira dalam mencegah ancaman orang dalam dalam organisasi. Beberapa penemuan penyelidikan ini amat penting untuk ahli akademik yang mencipta teori dan mendapatkan bukti empirikal yang berkaitan dengan keselamatan maklumat tingkah laku, sehingga tahap penemuan adalah dalam persekitaran yang berbeza. Daripada jumlah pemberat laluan piawai, keberkesanan tindak balas setakat ini merupakan faktor terpenting yang mempengaruhi keinginan orang dalam untuk mempertahankan organisasi mereka daripada risiko-risiko keselamatan maklumat privasi.

TABLE OF CONTENTS

CHAPTER 2 LITERATURE REVIEW

CHAPTER 3 CONCEPTUAL FRAMEWORK AND HYPOTHESIS DEVELOPMENT

CHAPTER 4 METHODOLOGY

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDIXES

LIST OF ABBREVIATION

VPN	Virtual Private Network
IT	Information Technology
IP	Intellectual Property
IRC	Internet Relay Chat
FTP	File Transfer Protocol
TTP	Trusted Third Party
SUT	System Under Test
CVC	Confidentiality via Camouflage
SDSC	Secure Data Sharing in Clouds
IDS	Intrusion Detection Systems
KDE	Kernel Density Estimation
SVM	Support Vector Machine
BBAC	Behaviour-Based Access Control
AVPS	Autonomic Violation Prevention System
CPU	Central Processing Unit
EBIAPM	Evidence-Based Intelligence Analysis Process Model
AD	Active Directory
BAIT	Behavioural Analysis of Insider Threat
DLP	Data Leakage Protection
DES	Data Exfiltration Surface
EML	Extensible Markup Language
PKI	Public Key Infrastructure
DLP	Data Loss Prevention

SC	System Calls
HTP	Hypertext Transfer Protocol
HLR	High Level Rules
SDD	Software Data Diode
SNAD	Specialized Network Anomaly Detection
PPI	Probabilistic Padding Identification
LIWC	Linguistic Inquiry and Word Count
AVPS	Autonomic Violation Prevention System
SIEM	Security Information and Event Management
UAM	User Activity Monitoring
AMT	Amazon Mechanical Turk
ITPM	Insider Threat Prediction Model
PMT	Protection Motivation Theory
TRA	Theory of Reasoned Action
TPB	Theory of Planned Behaviour
TAM	Technology Acceptance Model
UTAUT	Unified Theory of Acceptance and Use ofTechnology
SDT	Signal Detection Theory
Scenario-Based Model	Scenario-Based Model
IDT	Innovation Diffusion Theory
SCT	Social Cognitive Theory
SJT	Social Judgment Theory

CHAPTER 1

INTRODUCTION

1.1 Introduction

The purpose of this chapter is to present a broad overview of the research conducted in this study . In the beginning of this chapter, the background and motivation of this research is introduced. Next, the chapter provides the theoretical supporting of this research as well as outlining the context of this study . It is then followed by problems identified that drawn the direction of this work, research objectives and research questions, and the scope of the study. The following section will be outlining the construction of the thesis with description of the upcoming chapters .

1.2 Problem background

The traditional notions of cyber security has emphasized on protecting systems or technology against attack that arise from the external threats (Fawzi, 2014; Hansen, 2009; Srivastava et al., 2011). However this notion need to be rectified as it is becoming norms and apparent that there are great number of attacks comes from insider threat (Magklaras, 2006; Magklaras, 2010). In a latest study by Legg (2015), provides analysis of security circumstances regarding insider threat with the percentage of 58% (Legg, 2015; Randazzo et al. 2005).

Additionally, Li et al. (2019) note that a notable number of employees fail to comply to the information security regulations of their firms, while underestimating the information security dangers, due to a lack of cyber security awareness. This might increase as a result of inadequate security policy education and awareness (Li et al., 2019). These have the result of human mistake, which is responsible for more than 95% of accidents (Yusif & Hafeez-Baig, 2021). The vectors for each assault style clearly demonstrate that these occurrences are the result of unethical behaviour. Sending private information in a manner, for instance, that increases the possibility of delivery failure. But not all vectors seem to be related to user mistake, but rather to the usage mode itself. All attack methods appear to be an overall misuse of the right to access the computer system rather than a targeted assault on a particular permit (Walker-Roberts et al. 2019). Because of this, businesses should have an insider threat detection system that can identify and neutralise dangerous insiders before they continue to pose hazards. However, there is a lack of understanding in the realm of insider threats (Al-Mhiqani et al. 2020).

Despite cutting-edge research on insider threats, difficulties with validating and improving the detection models still exist because there is a lack of actual data from enterprises. Another significant obstacle in evaluating and creating insider threat detection systems is the paucity of genuine insider threat data (Al-Mhiqani et al. 2020). Additionally, the evaluation notes that the datasets that were generated artificially yet included in the surveyed publications weren't made particularly for insider threats. Furthermore, while some of these databases were obsolete, others did not include dangerous data (Al-Mhiqani et al. 2020). There is a need for more study since during an analysis interval some insider threat detection systems were unable to deliver real-time answers. A disadvantage of offline detection methods is that they are unable to support and respond to a log analysis in a timely manner (Al-Mhiqani et al. 2020).

Additionally, employees that are open-minded are more likely to attempt new things, which makes it easier for hackers to infiltrate their businesses since they leave behind personal information and digital traces. The tendency for people to be trusted can be a major obstacle to awareness campaigns against social engineering dangers. Individuals in an organization need to take physical and data security for themselves and their businesses more seriously (Yeboah-Ofori &Islam, 2019). The development of contemporary networks has fast surpassed these attempts, despite nearly two decades of study looking for ways to identify and avoid insider attacks. Therefore, victims continue to claim significant losses brought on by nefarious insiders (Liu et al.2018). This may be caused by one or more of the following factors: 1) existing solutions pay insufficient attention to the early indications of an arising malicious insider, most of which do not raise alerts until damaging behaviours have occurred; 2) most solutions rely only on a single audit data source, reducing insights into threats; and 3) conventional data analytics counts too much on domain knowledge in extracting features or establishing rules, reducing insights into threats (Liu et al.2018).

In addition, it has been demonstrated that a single individual's conduct may cause considerable and permanent damage. Insiders can harm an organization's goals and missions by causing this harm (Happ, 2017). Account for billions of dollars in yearly organizational income loss (Maasberg et al.2020). The severity and frequency of this issue in firms today are highlighted by current research, which offers clear proof of this (Barrios, 2013). The average worldwide cost of insider threats climbed by 31% in the previous two years to $11.45 million, and the number of incidents jumped by 47% in that period," according to a 2020 global study (Observer IT, 2020). The difficulty of insider threat (IT) may be better recogniZed and managed through event evaluation and analysis (Saxena et al.2020).

Organizations must recognize the importance of insider threats because the dangers involved might be dangerous. However, because the adversary is viewed as existing outside of the organization, companies are more worried about external dangers than internal ones. The lack of investment in insider security is proof of this. For instance, the State of Security study(PWC, 2014) reported that businesses only spend around 11% of their sales on security defenses explicitly geared at reducing insider danger. This is an insufficient amount of expenditure needed for the prevention and detection of these risks, given the level of risk involved. Likewise, if businesses think this threat is unimportant, they won't spend additional money guarding against it. For instance, the Ponemon poll revealed that just 44% of respondents thought their organization gave insider threats the highest priority, despite 61% of employees believing it to be a serious danger (Ponemon Institute, 2011). This highlights the reality that firms feel underprepared yet lack the drive to implement risk management. Additionally, organizations see the likelihood of an assault as minimal, which has a negative impact on any measures put in place to guard against insider threats (Saxena et al.2020).

Additionally, the Singapore Ministry of Health (MOH) lost sensitive records of 14,200 patients who had been diagnosed with HIV on January 29, 2019, six months after the Singhealth data breach, and those details were stolen and posted online. The culprit reportedly obtained access to the private documents by taking advantage of a personal connection with a Singaporean doctor who had granted access to the MOH's HIV register, in what may be called a "classic" insider attack. It was revealed in March 2019 that workers from Singapore government agencies' hacked login credentials had been exposed and were being sold on the dark web

(Hooi, 2019, p. 2). Additionally, there are methods and tactics that can be used to stop insiders from taking advantage of organisational weaknesses already present. If such individuals were already present, an organisation could then try to minimise the risk of insider infiltration by terrorists and other hostile actors (BaMaung et al. 2016). To manage insider risks from various aspects, such as purpose, nature of danger, or accessible audit data source, several plans and techniques have actually been presented (Liu et al.2018). The research states that 1) data exfiltration, 2) breaches of data integrity or availability, and 3) sabotage of ICT systems are the most often seen insider threats (C. I. T. Team, 2014). Technically, traitors and unintended offenders might carry out these threats immediately (Liu et al.2018). Organizations continue to deal with internal security events (PWC, 2016; Ponemon Institute, 2018, 2019). The authors write, despite the significant studies on the issue of insider's risk (Lebek et al., 2014; Siponen & Vance, 2014; Hovav & Putri, 2016; Soomro et al., 2016; Cram et al., 2017). For instance, some studies (Bertacchini & Fierens 2008; Gheyas & Abdallah 2016; Salem et al. 2008; Sanzgiri & Dasgupta 2016) just focus on detection methods, or there is a lack of a systematic approach to the classification of the literature (Azaria et al. 2014).

In addition, assaults that are fundamentally motivated by financial gain and sabotage that shows the connections between motivating variables rather than focusing on a single motivating component are the most often studied topics in academic and practitioner circles (BaMaung et al. 2016). It may often be challenging to determine the primary driving forces behind insider assaults. Indeed, there may not be a single driving force behind these situations, and in many instances, the driving forces may be numerous, highly dynamic, deliberate, or accidental (BaMaung et al. 2016). Insider attacks frequently include a second core reason that is connected to an individual's dissatisfaction with their place of employment and is, frequently, a result of that organization's unwillingness to acknowledge an individual's job-related successes (BaMaung et al. 2016).

Even still, Noonan and Archuleta discovered that there was no connection between employee dissatisfaction and the insider threat, concluding from their research that the great majority of angry employees do not really carry out assaults (Noonan & Archuleta, 2008). Nevertheless, according to Shaw & Fischer's research from 2005, nine out of ten insider attack cases studied illustrated significant issues within their employment, and in nearly all cases, those employees' demonstrated signs of dissatisfaction and personal problems 1 - 48 months prior to an attack (Shaw & Fischer, 2005). These conclusions are supported by Greitzer et al. (2012), whose research emphasises that dissatisfaction may be discovered via examining the behaviour of employees in their job, according to a poll of experts. In fact, the study found that those displaying hostility toward management and other employees, conflict, and general negativity were all tell-tale signs of potential dangers (BaMaung et al. 2016).

Furthermore, important conclusions from earlier studies on malicious insider threats highlight the necessity of widely based preventive and detection methods. Observable behaviours and personal variables are common indications of possible harmful insiders in today's risk management administrative and technical mitigation strategies (Maasberg et al. 2020). This is because illogical behaviour can be hazardous and unpredictable, it can be sparked by rage or irritation, and it might be driven by a lack of job fulfilment (Lahcen et al.2020). Additionally, the phenomenon of cyber security in any business may be broken down into two categories: technological considerations, which serve as the initial lines of defence, and non-technical human elements, which include behavioural human factors and organizational culture, which is mostly managerial (Pullin, 2018). The field of human factors focuses on fostering the best possible interaction between people and technology (Lahcen et al.2020). Additionally, motive, which is the reason behind a person's conduct and is indicative of whether a person will do an act or not, is what drives that action (West Group, 1999).

Empirical results indicate that the lowering motive is crucial for two reasons. First, since motivation is so powerful, those who have it but lack the resources and opportunities frequently set about acquiring them as required (Pendse, 2012). Second, it was challenging to stop motivated insiders from misusing information when incentive was a major motivator (Sarkar, 2010). Finally, insiders committed crimes because their desire was greater than their effectiveness (Noonan, 2018).

1.3 Problem statement

With regards to human beings in present day, network has been use vastly ranging from online banking to connected physical infrastructure. Network security which was once become optional has become necessity (Chakkaravarthy et al. 2018). Due to that matter, Information Communications Technology (ICT) systems, for instance, are facing accumulative number of security threats which caused by insiders (Liu et al. 2018). Though there was almost two decades of research conducted seeking techniques to detect and prevent insider threats, the expansion of modern networks has quickly overtaken these efforts (Liu et al. 2018). According to Moore (2016), attacks caused my malicious insiders are more challenging to identify compared to those external attackers. Furthermore, back in 2016, the trend of unintentional insider has been increased (Collins et al. 2016) until present. Due to that matter the motivation to cope with insider threat is very demanding and likely to grow (Homoliak et al. 2019). However, despite the fact that the threat rise by terrorism has gained widespread heading over a decade, it is opposite when it comes to penetration of organizations by 'terrorist' rising from insider and the possible dangers these individuals present has not been fully explored (BaMaung et al. 2016).

Regarding this malicious attack, it affected various sectors, economies, and organizations of the world with significant damage (Maasberg et al. 2020). Insiders has the ability to misuse their authorized access to critical systems and ultimately steal or modify data systems for malicious intent or financial gain. The targets not only towards private sector enterprises, but also towards government institutions and critical infrastructures for motives, ranging from monetary gains and industrial espionage to business advantage and sabotage. The damages from the insider attack can be devastating due to the fact that insiders have access to valuable information assets that are unavailable to outsiders (Saxena et al. 2020). Due to that matter, as said by scholars in literature, the most commonly seen insider threats are data exfiltration, violations against data integrity or availability, and sabotage of ICT systems (Liu et al. 2018).

There is also a significant and growing body of research in this area, however most PMT studies have replaced behavioural objective with security behaviour. There is a known gap between motivation and behaviour, despite the fact that behavioural goals and subsequent behaviour are often relatively closely related (Sheeran, 2002; Sniehotta et al., 2005). A study of the available data shows that motivation only approximates behaviour half the time (Sheeran & Web, 2016). This is a drawback of research using PMT as an explanation model in the security domain (e.g. Boehmer et al., 2015; Crossler et al., 2014; Herath & Rao, 2009; Johnston & Warkentin, 2010; Lee, 2011; Liang & Xue, 2010; Tsai et al., 2016).

The effectiveness of the threat versus coping messages, however, as well as whether the threat and coping aspects would be additive (to determine, for instance, if the two elements provided together would be more successful than each part offered alone), must be considered. Threat appeals rather than coping signals, according to some survey studies, are better indicators of effective security activity. (e.g. Shillair & Dutton, 2016). PMT was chosen because it enables the researcher to examine how each user's perceptions and protective reactions interact. For instance, not all PMT components can accurately forecast security behaviour. Another drawback that can be inferred from the academic literature is that PMT theories might not be a perfect fit for different models and cultures (Belanger & Crossler, 2019). However, despite the fact that PMT research has made significant progress in predicting security intentions, those studies are restricted since real-world activity was not assessed or monitored (Boss et. al, 2015).

Despite the PMT's ability to forecast security behaviours, decision-makers should be advised against putting all of their faith in it. First and foremost, the idea accounts for around 40% of the diversity of intents among persons. With a measuring reliability of about 0.8, surveys were able to explain between 60 and 70 percent of the variation. Therefore, there is a substantial amount of measurement error, and a considerable fraction of the observed variation is unanticipated. Second, not every time does an action match a purpose. For instance, what is possible and realistic also influences behaviour. Thirdly, there are opposing hypotheses that are equally plausible. For instance, planned behaviour is a simpler concept that describes about the same diversity of behaviours (Sommestad & Hallberg, 2013).

On how to make PMT-based communications, however, there isn't a lot of information accessible. For instance, coping appraisal is a better predictor of intentions to behave securely, but interventional research in the field of health indicates that it may be easier to improve a person's evaluation of information security risks than their assessment of coping mechanisms (Milne et al., 2000).

Previous PMT-based research has employed PMT as a variance model and postulated the simultaneous and independent influences of PMT components. One of the theories supporting PMT, the transaction-based model of stress or coping theory, asserts that decision-making proceeds progressively from primary to secondary appraisals (i.e., sequential rather than parallel effects), and that primary and secondary appraisals should be considered to be interdependent processes (i.e., interdependent rather than independent effects). Ignorance of the sequential and interrelated impacts helps to partially explain the inconsistent results shown in prior experiments. As an example, the conclusion that perceived severity and vulnerability are significant in certain studies but not in others (Zhao et. al 2018). In certain studies (Vance et.al 2012) and others (Posey et. al, 2015), the consequences of response costs are also found to be considerable.

Furthermore, providing solution for insider threat for all organizations can be a multifarious problem due to the complicated link between human behaviour and the combination of technical and non-technical aspects. For instance, the elements of outsourcing, globalization, and technology advancement makes the process of understanding and mitigating insider threats complex. Moreover, these elements can blur the line between traditional insiders and external adversaries which concerns as terrorists who may conspire with physical insiders to access a system and its assets. To be added with, according to Ponemon Institute survey of privilege users (Ponemon Institute, 2014) companies is having difficulty knowing if an action delivered by an insider is a justifiable threat which make this one of the biggest challenge in mitigating this issue. It is hard to detect malicious actions, unless organizations imposed high standard of security policies and controls in place within an organization (Saxena et al. 2020). Due to that matter, in terms of the security tools that most organization owned, it producing many false positives and do not produce enough contextual information. Also, high-tech tools including endpoint monitoring for detection are not widely used (Saxena et al. 2020). Conjunction with that matter, there are still problems to be solved for organizations regarding the insider threat as the expansive nature of attacks can occur at any exploitation point within the company (Saxena et al. 2020).

1.4 Research questions

i. What are the factors triggers insider attacker to have the intention to cause harm to organization's information system?

ii. What is the relationship between security behaviours and the appraisal process in Protection Motivation Theory?

iii. What are the degrees of relevance of these identified reflective factors to Protection Motivation Theory?

iv. How to develop framework based on the result synthesized from data analysis?

v. How to verify the applicability and usability of the proposed framework through expert judgement?

1.5 Research objectives

i. To identify factors trigger / motivate insider (attacker) to attack organization’s data.

This research objective stated in the purpose of finding the factors that contribute or well defined as the core motivation for insider in attacking organization’s Information System. The concept of motive has been introduced by (Campbell, 1985, p. 17), whereby they emphasized on the grounds of human behaviour. Motive, is by means defined as “any power; or unconsciously giving rise to behaviour, providing continuity and guiding it” (Turkish Language Association). Koçel, (2010, p. 619) stated that motivation is also defined as people’s action with contribution of wishes and desires to execute a specific purpose. To be added with, according to Maslow’s Hierarchy of Needs Theory (1943), individuals motivation are synchronized with their ranking needs in a hierarchy according to their level of importance (Brooks, 2006, p. 55). In addition, Maslow also stated that emphasizing these needs are crucial as it lead to the factor which defining the behaviour of an individual by having the stake that each behaviour originates from the efforts to resolve their specific needs (Koçel, 2010, p. 623).

ii. To determine the relationship between security behaviours and the appraisal process in Protection Motivation Theory.

This research objective seeks to define the user security behaviours. As suggested by research, often user’s security behaviour is developed by factors concerning on internal and external dimension to the individual.

There are few determining factor of security behaviours within the policy in studies (Ng et al., 2009; Workman et al., 2008). Therefore, the urge in exploring the research gap to identify elements of specific security behaviours in an employment sample is vital rather to continue of using globalized indicators of employees' security behaviour (Blythe, John (2015). In addition, despite the fact that past research has provided core fundamental in understanding security behaviour in workplace, however it is remains uncertain and unstated in which factors (e.g. internal and environmental) are most vital for security and to discover whether the organizational context plays a role in defining these factors. To be added with, the current literature has essentially focused on factors for the prediction of attitudes, intentions or behaviours. By all means, more references is needed in defining the gist of matters that influenced these factors within the workplace and how they may interchange in defining stages of different security behaviours (Blythe, 2015).

iii. To determine the degrees of relevance of these identified reflective factors to Protection Motivation Theory.

This research objective seek to find the validity of the framework.

iv. To develop framework based on the result synthesized from data analysis. Six constructs (Crossler, 2010, Burns, 2017, Herath, 2009, Pahnila, 2012, Ifinedo, 2013) are included in the appraisal process along with PMT, but it is evident from the findings that the threat appraisal construct scores highly on Perceived Security Vulnerability and Maladaptive Reward while the coping appraisal construct scores highly on Prevention Cost. These four elements, along with Fear and Protection Motivation, make up the framework's foundation, which is based on discoveries and readings. (an additional construct that excludes reflective aspects and threat appraisal). According to the findings, which were mentioned above, these six components interact with one another to form the framework's core.

v. To verify the applicability of the proposed framework through expert judgement.

According to Escobar-Pérez & Cuervo-Martnez (Pérez & Martnez, 2008) (p. 29), content validation through expert judgement refers to an informed opinion from people with experience in the field who are regarded by others as qualified experts and who are able to offer information, evidence, judgments, and assessments. Evaluation by expert judgement is the process of gathering feedback on a tool or multiple people's perspectives on a single component (Cabero & Almenara, 2013). Most often, content validations are done as part of the test design process or as part of standardising and translating an instrument for usage in a new culture. Specialists are crucial in both cases for identifying, incorporating, and/or altering the necessary components (Garrote & Rojas, 2015).

1.6 Operational definition

There are few concepts with phrases and abbreviations that are used throughout this research:

Insider: An insider is someone who is familiar with the organizations IS structure and has allowed access to it. They also understand the underlying network topologies of the organization's IS. .

Insider Threat: An insider's activity that disrupts or poses an undesirable danger to an organization's data, procedures, or resources.

Intentional Insider Threat: According to academic definitions, an intentional insider threat occurs when a person of trust, such as an employee, contractor, consultant, or vendor, with legitimate access to a company tries to cause harm by engaging in counterproductive behaviour that will lead to the loss, disclosure, or destruction of that company's information, resources, assets, or reputation (Bedford 2019, 136).

Protection Motivation Theory: The notion of protection motive was created in order to explain the appeals to fear. According to the protection motivation theory, people decide how best to defend themselves based on four considerations: the perceived seriousness of a threat, the perceived likelihood that it will occur, or vulnerability, the effectiveness of the suggested preventive behaviour, and the perceived self-efficacy.

Threat Appraisal: An evaluation of vulnerability made cognitively that may or may not be connected to the powerful emotional response to impending danger (the "fight-or-flight" response, which is triggered by neuronal activity in the amygdala and is marked by a significant surge of adrenaline)

Perceived vulnerability: Refers to a person's judgment of the likelihood that they may face a threat.

Perceived Severity: Evaluates the severity of the effects on a person if the threat is successful.

Coping Appraisal: A concurrent cognitive mediation process in which the message recipient evaluates both the effectiveness of the suggested reaction and his or her own capacity to deal with the danger.

1.7 Research scope

This study focuses on the organizational level, where employee responsibilities and departmental functions dictate the breadth of access. The entire organization, particular and specified organizational functions, specific and identifiable organizational divisions, or one or more functions within a set of organizations may all fall under the purview of a management system. Sales, compliance, construction, delivery, installation, support, service, and maintenance of communication services in accordance with client needs, as well as the production, design, and supply of architectural membrane structures excluding installations, might all fall under this category. Additionally, heavy hauling, civil construction, plant hire, bulk earthmoving, and workshop operations.

1.8 Significance of Research

Computers are now more ingrained in both daily life and business processes. Bad actors are increasingly targeting them as well. The time when a burglar needed to physically enter a building to steal confidential business information or individual information is long past. For more than three decades, cybercriminals have used networked computers to get past cyber defences and erase, change, or delete digital information (Elmer-DeWitt et al., 1983; Incognito Forensic Foundation Lab, 2017). Many hackers use cyber techniques that have been well-known to information security specialists for many years and have relatively simple defence mechanisms, however some cyber-attacks are highly complex and demand large resources to counter. In 2016, consumers failed to back up important data and cyber-attacks using default passwords caused interruptions and havoc (Berr, 2017; Krebs On Security, 2016; York, 2016). Industry experts are not the only ones with expertise of cyber security; consumer-oriented periodicals frequently cover cyber tales and security solutions. The public has access to the material, hence limitations in implementation do not seem to be the result of ignorance. However, as seen by newsworthy data breach stories, healthcare industry leadership has not put in place necessary security measures. Industry professionals and consumer magazines can better advise people and corporate computer users to better protect themselves against computer assaults and secure their sensitive information by understanding what prevents the use of fundamental cyber security solutions.

As for the significance of research, it is projected that the result of the study will increase the level of security and awareness among employers and employees which can be contributed in information security field. Furthermore, it is expected that the research would increase the understanding of the issues and concerns in Information System Security. In addition, the research could enhance the understanding of the relevance of these identified factors and their attractions with each other. It is hoped that the framework developed from this research could help in decreasing the insider threat occurred in organization.

In addition, an insider threat prevention framework that will be developed from this research can be used to prevent as well as decrease threats that occurred in organizations as well as promoting an environment that will lead to the understanding and creating a security culture within any organization. Furthermore, a significant increase in the body of knowledge will result to assist employers and employee to understand the importance of information security. To be added with, an extension of knowledge about information security culture will help address the paucity of information security research that exists with respect to developing countries emerges.

1.9 Thesis Layout

This thesis consists of 6 chapters. The first chapter provides an outline of the research whereby it consists of its background, aims, problem research, research objectives, research questions and research scope .

Chapter 2 consists of in-depth investigation conducted for insider threat in preventing this issue in organization . A systematic review protocol is structured for literature review to analyze the challenges and as well as developing taxonomy for the research articles in the area of insider threat .

Chapter 3 consists of the development of the framework itself. The discussion begins with an overview of the study's history and setting. After that, we revise factors in light of previous studies on the factors that affect employee’s motivation to protect organization’s data, before introducing the framework for early research with PMT. In supporting to this chapter, the tittle has mentioned development of work therefore this chapter needs to be existent regarding to that matter.

Chapter 4 concerns the methodology and the research design of this doctoral research . This chapter describes the sampling, data collection procedures, and analysis techniques . Afterwards it discuss the quantitative data analysis, including survey rationale, survey content, analysis approach, questionnaire development, data collection method, measurement scale, sampling, analysis technique and data validation .

Chapter 5 discusses and presents results of the descriptive statistics analysis based on the questionnaire survey. This chapter presents the survey respondents' profiles, followed by the screening of the survey data to ensure that it is compatible with the ensuing multivariate statistical analysis, such as Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equation Modelling (SEM). Thereafter, the first findings from the survey are discussed. This chapter also covers the measurement scale analysis findings, including reliability scale analysis findings, which helped to assess the measurement scales used in the survey questionnaire's internal consistency. The next section discusses structural equation modelling (SEM), confirmatory factor analysis (CFA), and exploratory factor analysis (EFA). The right amount of factors (also known as factor structures) for any model design may be found with the use of EFA. The validity of each concept is further strengthened by CFA's confirmation of the identified factor structures. Additionally covered in this chapter is the topic of model testing. On the basis of the findings of the measurement scale analysis, the model evaluation is carried out in steps. The SEM overviews employing covariance-based techniques, such as Analysis of Moment Structures, are covered in this chapter (AMOS). The evaluation of the measurement model is next addressed, followed by the findings of the model measurement.

Chapter 6 represents in a nutshell of this thesis. It starts with an overview of the research project, followed by the research problem and research questions . Then the contributions of the research are presented as well as discussing its implications for academic and practitioners . This chapter continues by discussing the limitations of this research and future research opportunities .