© Sungai Siput Community College, Ministry of Higher Education, Malaysia

JTH

https://jthkkss.com/
e-ISSN 2805-4431
DOI: https://doi.org/10.53797/jthkkss.v2i1.3.2021

A Confirmatory Analysis of the Prevention of Insider Threat in Organization Information System

Abu Bakar, Rahimah[1], Rahmatullah, Bahbibi[1*], Munastiwi, Erni[2] & Dheyab, Omar[3]

[1]Faculty of Art, Computing and Creative Industry, Sultan Idris Education University, 35900, Tanjung Malim, Perak, MALAYSIA

[2]Faculty of Education and Teacher Training, Islamic State University Sunan Kalijaga Yogyakarta, 55281 Yogyakarta, Central Java, INDONESIA

[3]Departmant of Computer Science, Baghdad University, Baghdad Governorate, IRAQ

*Corresponding author email: bahbibi@fskik.upsi.edu.my

Available online 19 May 2021

Abstract: Many issues related to insider threats in organizations have been debated ever since. Although insider attacks may not occur as frequently as external attacks, they have a higher success rate, go undetected, and pose a much greater risk than external adversaries. About that, many mechanisms have been proposed to be an initiative to protect data from outside attacks. However, those mechanisms could not protect data from authorized users who may misuse their privileges. Due to those circumstances, developing mechanisms that protect sensitive data from insiders becomes a pitch demand to prevent harm caused by malicious insiders. The method of this research is the quantitative method using a questionnaire. The findings have contributed to developing a framework that will be used to prevent insider threats in an organization in the future.

Keywords: Insider threat, insider attack, protection motivation theory, confirmatory factor analysis, information system

1. Introduction

The traditional notions of cybersecurity have emphasized protecting systems or technology against attacks arising from external threats (Fawzi et al., 2014; Pelechrinis et al., 2011; Probst & Hansen, 2009). However, this notion needs to be rectified as it is becoming the norm and apparent that many attacks come from insider threats (Magklaras & Furnell, 2010; Magklaras et al., 2006). A recent Legg et al. (2015) study shows that 58% of reported security incidents resulted from insider threats.

According to the 2011 Cyber-security Watch survey (Srivastava et al., 2011), 58% of cyber-attacks on organizations are attributed to outside threats, and 21% of attacks are initiated by their employees or trusted third parties. Besides, as mentioned (Randazzo et al., 2005), many incidents were planned. This included individuals who had already been involved in the incident and potential beneficiaries of the (Silowash et al., 2012) insider activity (74%), co-workers (22%), friends (13%), and family members (9%).

Many organizations fail to detect an insider threat that can cost billions of pounds per year and cause severe damage to the organization, much of which goes unreported, so the true extent of the problem is still unknown. An 'insider' is anyone with privileged access (e.g., an employee, contractor, client or business partner) to an organization's data, systems or infrastructure, and an 'insider threat' is an insider that intentionally abuses this access for some gain. Although insider attacks may not occur as frequently as external attacks, they have a higher success rate, can go undetected, and pose a much greater risk than external adversaries (Althebyan & Panda, 2007; Chinchani et al., 2005).

The cost of security breaches can reach up to $5.4 million in some organizations, whereas security attacks are causing organizations an average cost of $591,780 per attack. Info Security Magazine has reported that, globally, IS

*Corresponding author: bahbibi@fskik.upsi.edu.my expenditures have reached $55 billion, and it projects that, in 2016, the security expenditures around the world will reach up to $86 billion (Alaskar et al., 2015). Therefore, we aim to investigate and identify the factors that contribute to insider threat in the organization and develop a framework that could be used to prevent insider threat.

2. Literature Review

A central goal of managing information systems is the assurance of the information's security which its confidentiality, integrity, and accessibility, which comprises a plethora of activities to, among other things, implement and maintain technical, behavioural, and economic controls to prevent and deter threats arising from internal and external sources which may originate from human or non-human sources (Warkentin et al., 2016). Extensive research has pointed to the insider, typically the employee, as a primary source of threat to the information system's security. Employee actions that threaten the security of organizational information resources may be accidental or volitional but not malicious (Warkentin et al., 2016).

A systematic review has been done regarding this research to retrieve what factors trigger insider threats to commit and attack an organization's data. To identify potential factors that influence the successful implementation of strategies, we first identified as many factors as possible that influence the implementation of security in organizations (Park et al., 2010). This phase was necessary because extracted factors will be used to build an architecture of ISS strategies, which implies that they need to be examined using organizational, architectural, and information systems standpoints (Park et al., 2010). An initial examination of factors in the literature review reveals that factors can be grouped based on their features and roles (Park et al., 2010).

There are 22 factors identified in the literature review. However, according to the enclosure based on literature, factors that motivate an insider to launch an attack towards the information system would be human, organisational, cultural, psychological, demographic, and personal characteristics factors. This is based on the number of works of literature by scholars. The survey includes organizational, human, demographic, cultural, economic, structural, operational, technological, environmental, and psychological factors.

Theory is fundamental to research; without it, research does not exist. Based on the literature, few theories have been used relating to insider threat. Scholars proposed many theories from various areas. Meanwhile, this research has identified behavioural theories, such as the Theory of Reasoned Action, General Deterrence Theory, and Protection Motivation Theory, which explain how behaviours are shaped.

Moreover, researchers' arguments indicate that more than technology is needed to ensure security and have started to pay attention to the human aspect of security (Ng et al., 2009; Workman et al., 2008; Woon et al., 2005). However, as stated by Liang (2010), knowledge about user security behaviours still needs to be completed.

In addition, IT security research has studied perceived susceptibility and severity with inconsistent results. The fact reveals that perceived vulnerability (susceptibility) does not predict whether individuals will execute network security (in their home), but perceived severity does (Woon et al., 2005). Meanwhile, according to Ng et al. (2009), perceived susceptibility affects users' email security behaviour, but perceived severity does not. On the other hand, (Workman et al., 2008) stated that perceived vulnerability and severity affect user IT security behaviour (Liang, 2010). Furthermore, more creative research approaches are needed in order to retrieve facts on understanding the cognitive and affective processes of both terms "white hat" and "black hat" IS security policy violators (Mahmood et al., 2010). The suggestion of the present study concerns the term "white hat" (employee, student, contractor, agent, customer), which is projected by organizations to indulge with numerous IT security policies and procedures, including devoting in protective behaviour such as making a backup of important data, avoiding suspect emails, encrypting mobile data and other activities (Warkentin et al., 2012).

Besides, malicious IT could be an agent continuously invading systems that cause malevolent changes (Liang, 2010). Added, based on prior research conducted by Weinstein (1993), Maddux and Rogers (1983), and Bandura (1982), people tend to consider a safeguarding measure by considering how it effectively counters the IT threat, concerning costs they are about to engage, and how convinced they feel about using it (Liang, 2010). Furthermore, as stated by the Technology Threat Avoidance Theory (TTAT), users' emotional disturbance is often triggered by the scary prospect of the threat when the threat level is high. This situation automatically generates a problem-focused coping to cope with the objective threat and utilize emotion-focused coping to mitigate the user's emotional uneasiness (Liang, 2010).

Moreover, various forms of malicious IT have continuously jeopardized the security of contemporary computing environments. Theory-based empirical research addresses that computer users' voluntary IT threat avoidance behaviour needs to be improved. This is supported by most existing security research on individual behaviour focuses on organizational settings, whereby threat avoidance behaviour is mandatory (Liang, 2010).

This comes to the enclosure based on literature; Protection Motivation Theory (PMT) has been presented as one of the most influential theories in health social sciences for predicting an individual's intention to engage in protective manners (over 15 theories identified). However, its importance and influence have also been proven in information security compliance behaviour in recent years. The integration of the Theory of Planned Behaviour (TPB) with the Protection Motivation Theory (PMT) was inspected by Ifinedo (2012) to understand information security policy compliance. Overall, his results from the business managers and IS professionals suggested a significant influence of

PMT over TPB. Moreover, Vance et al. (2012) and Siponen et al. (2006) also investigated the integration of protection motivation theory (PMT), the Theory of Reasoned Action (TRA) and cognitive evaluation theory (CET); to explain employees' adherence to information security policies. His theory-based model presented significant results with the role of protection motivation theory (PMT) in actual compliance with information security policies. Therefore, it is assumed that protection motivation as a countermeasure to security risks in Malaysian institutions can bring employees closer to information security policy compliance (Ahmad et al., 2016).

3. Methodology

Researchers have employed PMT to assist in understanding individuals' protective intentions and behaviours in varied motivational settings (Floyd et al., 2000; Milne et al., 2000), including IS security research (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Herath & Rao, 2009; Lee & Larsen, 2009; LaRose et al., 2008; Workman et al., 2008; Woon et al., 2005).

PMT can explain security behaviours outside of a corporate setting, providing a theoretical explanation as to why people perform specific countermeasures to detect and prevent computer threats, ultimately deterring continued attacks on computer systems. The premise of PMT is that information is first received (sources of information), which leads to an evaluation of it by the person receiving that information (cognitive mediating process), and finally to the person taking some action based on the information received (coping mode). Sources of information are the input variables to the model and include environmental and intrapersonal sources. There are two types of cognitive mediating processes: the threat appraisal process and the coping appraisal process. The threat appraisal comprises the threat perception (severity) and (vulnerability) of continuing with the maladaptive response. The coping appraisal process consists of the individual's confidence that a coping response will reduce or mitigate a security threat (response efficacy) and that he believes he can perform the given response (self-efficacy), but that the cost of performing such an action is not too high (prevention cost) (Crossler, 2010).

Previous IS security studies have used PMT to assess the motivation related to various security-related intentions and behaviours. For example, PMT has been applied to the protection of personal resources from information security threats by motivating behaviours related to the adoption of home wireless security systems (Woon et al., 2005), anti-spyware/anti-malware software on personal computers (Lee & Larsen, 2009), and location-based services (Junglas & Watson, 2008). Researchers have also effectively tapped PMT to explore employees' intentions to protect organizational resources by adopting virus-protection software at work (Lee & Kozar, 2008), performing basic computer security operations at work (e.g., updating passwords, securely backing up essential files, and updating virus protection software) (Workman et al., 2008), and complying with organizational information security policies (Herath & Rao, 2009; Siponen & Willison, 2009). PMT includes the recognition that only some responses to organizational threats are adaptive. This may result from insiders' beliefs that the organization is inflexible, the threat is not convincing, or the personal benefit of failing to overshadow adaptation (termed maladaptive response) (Burns et al., 2017).

In the Information System (IS) context, the PMT has been used to examine users' protective behaviour in an online transaction, employee's awareness of organizational information security policies and individual use of security software. However, only a few studies found applying the PMT to explain users' protective behaviour associated with information disclosure (Salleh et al., 2012). According to Maddux and Rogers (1983), Fear influences behaviour only indirectly through appraisal of treatment severity, as the state of fear arousal may explain PMT variables' influence on motivation, according to the PMT. In addition, perceived vulnerability elicited Fear, which contributed to exercise intentions, whereby fear arousal was a mediator in one prediction study. This suggests that threat appraisal has limited influence on protection motivation if Fear is not aroused (Plotnikoff & Higginbotham, 2002).

Besides, the PMT interventions used persuasive communications; this is still being determined whether behavioural, experiential, or other innovative techniques would be effective (Woon et al., 2005). According to Maddux and Rogers (1983), PMT measures a person's coping behaviour when a threatening event is informed to them. This act refers to a person's willingness to perform a recommended behaviour whereby the coping response directly influences this behaviour. The coping response is the result of the person's evaluation of the threat appraisal and coping appraisal.

About this theory, we are expanding this theory with identified factors that trigger insider threats in an organization, traced from the previous literature review. Fig. 1 of the model is shown. The identified factors are the factors that motivate and trigger insiders to commit an attack on the organization. These factors will go through threat appraisal and coping appraisal. In threat appraisal, threat vulnerability, severity, and maladaptive rewards exist. In threat vulnerability, the insider will go through a stage where they assume the organization's information and information systems are vulnerable to security threats. In threat severity, insiders will go through a stage where they assume the threat to the security of their organization's information and information system is severe. In maladaptive rewards, the insider will go through a stage where they assume they will receive personal rewards for purposely not protecting their organization's information and information systems from security threats. They would also feel a sense of internal satisfaction for allowing information security threats to harm their organization. As in coping appraisal, there are response costs, security self-efficacy, and security response efficacy. In response to cost, the insider will go through a stage where they assume the inconvenience of implementing recommended security measures to protect their organization's information and information systems exceeds the potential benefits. In security self-efficacy, insiders will go through a stage where taking information security precautions to protect their organization's information and information systems is easy. In security response efficacy, insiders will go through a stage where they assume employee efforts to keep their organization's information and information systems safe from information security threats are effective. After going through threat appraisal, insiders will go through the fear stage. In this stage, insiders will go through a stage where, when thinking about the security threats to their organization's information and information system, to what extent they will feel. Fear involves physiological which trigger cognitive, affective, and behavioural responses. Hence, with the fear element, the Information system will be secured. In addition, after coping appraisal, insiders will go through a stage where they feel intended to protect their organization from its information security threats. Hence, with this theory, the Information system will be secured.

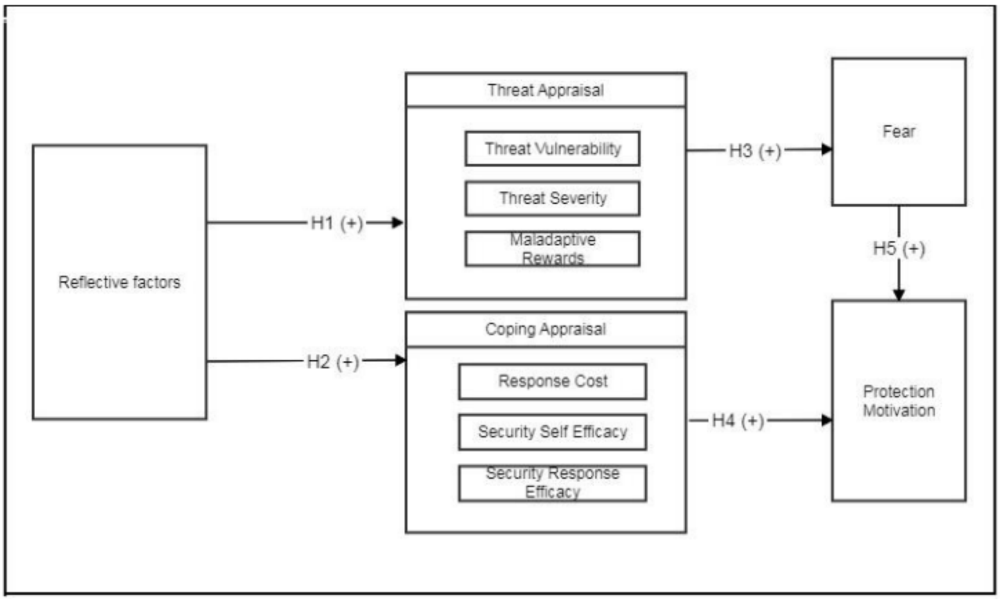

Fig. 1: The framework for preventing insider threat

Based on the objective and factors influencing this study, several hypotheses have been made to determine the result of this research. In PMT, threat appraisal is described as an individual's assessment of the level of danger posed by a threatening event (Woon et al., 2005; Maddux & Rogers, 1983). This appraisal is composed of perceived vulnerability and perceived severity. The perceived vulnerability could be related to an employee's assessment of the probability of threatening events (Gundu & Flowerday, 2013). In this research, we refer to factors in organizations such as human factors (i.e. Lack of attention), and organizational factors (i.e. management practices) having been influenced by threat appraisal. Perceived severity implies the severity of the consequences event (Gundu & Flowerday, 2013). Perceived severity will positively affect security compliance concerning safe computing in the organization; however, individuals who consider themselves immune to security threats are more likely to ignore security measures at work (Lacey, 2010; Herath & Rao, 2009; Pahnila et al., 2007). It is also reasonable to expect that individuals who perceive the high risk to their organization's information system resources will be more likely to adopt protective behaviours (Pahnila et al., 2007; Woon et al., 2005). Therefore, we come out with this hypothesis: H1 Reflective factors positively influence Threat Appraisal.

Coping appraisal involves a process that provides a subjective cost-benefit analysis of the potential benefits of proposed protective measures to prevent or mitigate criminal threats (Clubb & Hinkle, 2015). Therefore, we came up with this hypothesis: H2 Reflective factors positively influence Coping Appraisal.

Fear appeals are designed to increase the message recipient's perceptions of a threat's severity and one's weakness or vulnerability to it (known as "threat appraisal"), while also seeking to boost the recipient's efficacy levels by recommending a response (response efficacy) that is said to be easy to perform (self-efficacy) (Warkentin et al., 2012). For fear appeals to be effective, the message must manipulate the neural regions responsible for cognitively processing perceptions of threats and efficacy (Warkentin et al., 2012). On the other hand, threat appraisal is a cognitive assessment of vulnerability which may or may not be associated with the intense affective response to immediate danger (the "fight" or "flight" response) is activated by neural activity in the (amygdala), and which characterized by a massive release of adrenaline) (Warkentin et al., 2012). Therefore, we came up with this hypothesis: H3 Threat Appraisal positively influences Fear.

According to Gundu and Flowerday (2013), in coping appraisal, self-efficacy emphasizes the employee's ability or judgement regarding their capability to cope with or perform the recommended behaviour. This research context refers to the skills and measures needed to protect the organization's information assets (Pahnila et al., 2007; Woon et al., 2005). Regarding response efficacy, this factor relates to the belief in the perceived benefits of the individual's action (Maddux & Rogers, 1983). This juncture refers to compliance with information security as an effective mechanism for detecting a threat to the organization's information assets (Gundu & Flowerday, 2013). Regarding response cost, this factor emphasizes perceived opportunity costs in terms of financial, time and effort expended in adopting the recommended behaviour (Gundu & Flowerday, 2013). Response efficacy will have a positive effect on information security policy. In other words, when employees perceive a threat, they often adjust their behaviour in response to the level of risk and determine if they are willing to accept the risk (Workman et al., 2008; Milne et al., 2000). Therefore, an individual's perceived severity tends to be positively linked to their intentions to follow protective actions (Pechmann et al., 2003). Thus, we came up with this hypothesis: H4 Coping Appraisal positively influences Protection Motivation.

An emotional response to a threat that expresses, or at least implies, some danger is called Fear. Fear significantly affects behaviour, leading them to seek ways of removing or coping with the threat and the danger for most people (Tanner et al., 1991). An appeal communication that involves Fear usually attempts to influence or persuade through the threat of impending danger or harm (Rogers, 1975). In addition, through experimental findings, fear appeals are generally effective in producing an attitude change (Maddux & Rogers, 1983). Thus, we come out with this hypothesis: H5 Fear positively influences Protection Motivation.

This phase of research is concerned with the validity of the constructs themselves. It is vital to ensure the observed variables' validity and capture the essence of the desired latent variables before analyzing the model and its path. A survey instrument was developed to test the indicators chosen for the proposed latent variables. Items were measured using a 4-point Likert scale consisting of "Strongly Disagree", "Disagree", "Agree" and "Strongly Agree". The study was conducted and distributed on a sample of 305, and 205 were received. Respondents held positions identified as "Managerial" with 2%, "Technical" with 78%, and "Professional staff" with 20%. Further, company size was identified as medium, with 90.7 % employed by a company with less than 10000. As the focus was the validation of the factors synthesized from the literature, collected data was analyzed using Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), and Structural Equation Model (SEM).

4. Results and Discussion

To use survey-based methodology, a key concern is usually regarding assuring the scale's reliability. A popular test for scale reliability is Cronbach's alpha, which determines the internal consistency of items in a survey instrument to gauge its reliability. The Cronbach's alpha of the instrument was calculated as .85, exceeding the .70 found to be an acceptable reliability coefficient.

The data was loaded in SPSS AMOS 22. Table 1 depicts the path diagram generated by SPSS and SPSS AMOS. Regarding EFA, rotated factor loadings identified four factors which accounted for 84.25% of the total variance. The eigenvalues extracted for the four components are 9.113 (Component 1), 4.573 (Component 2), 1.905 (Component 3), and 1.259 (Component 4). As for the % Variance, the result shows 45.563 (Component 1), 22.867 (Component 2), 9.526 (Component 3), and 6.297 (Component 4). In terms of cumulative variance explained, the result shows 45.563 (Component 1), 68.430 (Component 2), 77.956 (Component 3), and 84.253 (Component 4). In addition, four factors derived from 20 variables are a) factors that influence insider threat to attack organization's data: Organizational factor (10 variables, component 1); b) factors that influence insider threat to attack organization's data: Prevention cost (5 variables, component 2); c) factors that influence insider threat to attack organization's data: Maladaptive reward (4 variables, component 3); and d) factors that influence insider threat to attack organization's data: Security practice (1 variable, component 4).

Table 1: Rotated factor loadings of the research framework constructs

		Component			
		1	2	3	4
Work Environment	OF3	.954			
Workload	OF4	.941			
Management practices	OF1	.933			
Policies	OF2	.933			
I am at risk for losing information or files on my computer	PSV1	.932			
I will likely lose information or files on my computer	PSV2	.926			
When thinking about the security threats to your organization's information and information system, to what extent do you feel. Fear (1); Frightened fear (2); Nervous fear (3); Anxious fear (4); Uncomfortable (5)	F1	.834			

Table 1: Rotated factor loadings of the research framework constructs (Continued)

		Component			
		1	2	3	4
The inconvenience of implementing recommended security measures to protect my organization's information and information systems exceeds the potential benefits	PC4	.820			
Backing up data on my computer requires a significant amount of time	PC2	.802			
Backing up data on my computer requires significant financial cost	PC1	.677			
The negative side effects of recommended security measures in my organization are greater than the advantages	PC7		.921		
The negative impact on my work from recommended security measures to protect my organization's information and information systems is greater than the benefits gained from the security measures	PC5		.899		
It is likely that I would receive personal rewards for purposely not protecting my organization's information and information systems from security threats	MR1		.872		
Recommended security measures are so much of a nuisance that I think my organization would be better without them	PC6		.708		
I could be rewarded personally for not protecting my organization from information security threats	MR2		.583		
I would feel a sense of internal satisfaction for allowing information security threats to harm my organization	MR4		.841		
I could be rewarded financially for choosing not to protect my organization's information and information systems from security threats	MR5		.830		
I believe others would be willing to reward me financially for intentionally failing to protect my organization's information and information systems from security threats	MR6		.793		
I would receive personal gratification for purposefully not protecting my organization from its information security threats	MR3		.759		
Backing up data on my computer requires significant cognitive effort (brainpower)	PC3		.829		
Eigen Value		9.113	4.573	1.905	1.259
% Variance		45.563	22.867	9.526	6.297
Cumulative Variance Explained		45.563	68.430	77.956	84.253

OF: Organizational factor; PSV: Perceived security vulnerability; PC: Prevention cost; MR: Maladaptive reward; F: Fear. Cronbach's Alpha= 1.00 Yellow highlighter indicates factor loading

Concerning CFA shown in Fig. 2, the sample covariance matrix was analyzed using the maximum likelihood minimization function. Maximum likelihood was chosen because it allows for a statistical evaluation of how well the factor solution can reproduce the indicators' relationships. The goodness of fit was evaluated using the Standardized Root Mean Square Residual (SRMR), Root Mean Square Error of Approximation (RMSEA) and its 90% confidence interval (90% CI), and the Comparative Fit Index (CFI). Acceptable model fit was defined by the following criteria: RMSEA > .06 with 90 % CI .95. Multiple indices were used because they provide different information about model fit (i.e., absolute fit, fit adjusting for model parsimony, fit relative to a null model); used together, these indices provide a more conservative and reliable evaluation of the solution. The selected goodness-of-fit indices provided mixed results for model fit. The model appears to have a fit of df =146, GFI=.461, AGFI=.299, NFI= .588, TLI=.529, CFI= .598, IFI= .599, RMSEA=.316.

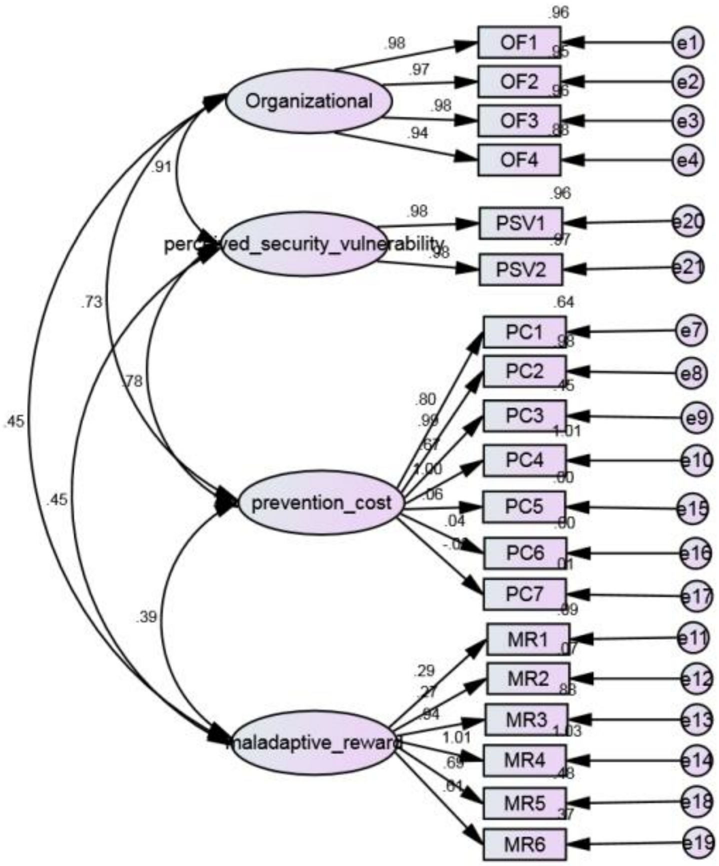

Fig. 2: CFA Model for factors influencing insider threat prevention framework

Furthermore, results of the path analysis were retrieved as shown in Fig. 3, whereby a significant positive relationship was found between Organizational factor (reflective factor) and Perceived security vulnerability (β = 0.461, p < .001) and the value of Organizational factor (reflective factor) and Maladaptive reward (β = 0.250, p < .001), therefore H2 is supported. The perceived security vulnerability (threat appraisal) was found to be significant with Fear (β = 0. 369, p < .001) and Maladaptive reward (threat appraisal) and Fear (β = 0.034, p =.014); therefore, H3 is supported. Prevention cost (coping appraisal) was insignificant with Protection motivation (β = 0.014, p = .683); therefore, H4 is unsupported. Fear and protection motivation (β = 2.564, p < .001) was significant; therefore, H5 is supported.

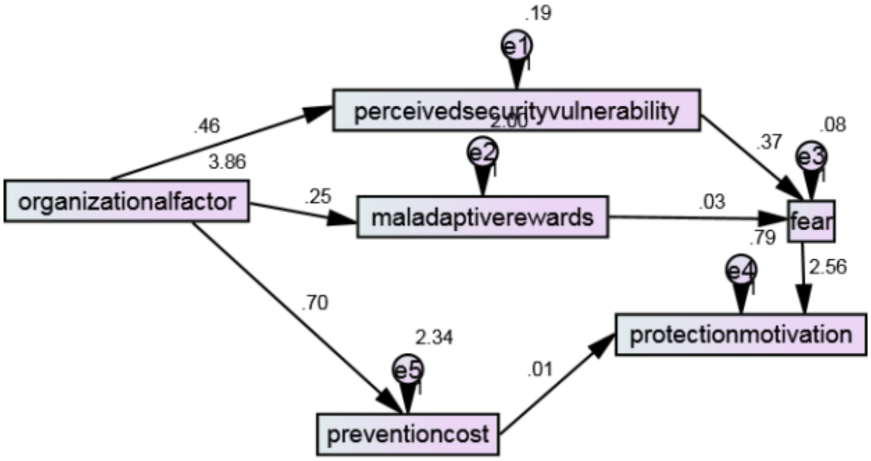

Fig. 3: Standardized path coefficients for the hypothesized model

The findings show that all the predicted factors based on literature (organizational, human, demographic, cultural, economic, structural, opportunity, technological, environmental, and psychological) are contributing to insider's motive in attacking the organization's data (descriptive analysis). After SEM analysis had been conducted, the organization factor was found to be most fit in this framework. Organizational factor (Reflective factor) and Perceived security vulnerability have a value of (β = 0.461, p < .001) and the value of Organizational factor (Reflective factor) and Maladaptive reward (β = 0.250, p < .001), which found to be having a significant value. Concerning the factors that trigger insiders to attack organization data, the findings indicate that the factor that influences and is positively associated with the appraisal process is an organizational factor.

5. Conclusion

This research was conducted in response to the need for more empirical studies to prevent insider threats in organizations. To achieve the objective of this research, an insider threat prevention framework comprising reflective factors (factors that trigger and motivate malicious acts in the organization) and constructs in PMT was developed based on an extensive literature review. The framework has undergone assessment and refinement using a series of quantitative techniques, specifically Exploratory Factor Analysis (EFA), Confirmatory Factor Analysis (CFA), as well as Structural Equation Modelling (SEM). These techniques were conducted based on data obtained from the questionnaire survey of Malaysian organizations. The current study also contributed to existing knowledge by providing a valid and reliable insider threat prevention framework as an alternative to providing an initial understanding of factors that motivate malicious acts in cybercriminals. The framework could serve as an alternative for Malaysian organizations to prevent cybercriminals. Finally, the research ends with future work recommendations that may help researchers extend and enhance this research's findings.

Providing a reliable and valid insider threat prevention framework is the primary benefit. This research could help academic researchers identify gaps in the information security field, focusing on insider threats and identifying further research needed. This includes examining factors related to various other Asian countries. Therefore, the current research assists in filling a gap in the information security field. Furthermore, this framework could be replicated in other environments. This research's framework provides a reference point for a wide range of empirical studies that could be conducted in order to test the framework. In addition, the research model in the current study could be a cornerstone as guidance for future empirical researchers in the information security field. The constructs in this research can be used as a dependent variable in other studies.

This research presents a quantitative assessment that information security managers and practitioners can use as an alternative to security awareness to prevent insider threats in organizations. The instruments presented were designed with academic thoroughness and have been tested in several phases with empirical data. This framework was statistically tested for validity and reliability with 205 Malaysian participants representing diverse industries, types, sizes, and roles in Malaysian organizations. This research helps information security managers develop essential aspects of information security as an alternative practice in preventing malicious acts by cyber criminals. The framework also provides management with practical information security approaches.

Furthermore, this research could minimize employees' threats to protecting an organization's information assets. The insider threat prevention framework facilitates what factors could be enlightened to prevent the malicious act. Management can assist in directing humans' interaction with information security as an alternative to protecting information assets.

Future research may include retrieving any other factors that trigger and motivate malicious acts in other diverse environments. Researchers could also expand this framework to other developing countries in the region, such as other Asian countries, and collect variables from various data sources to minimize biased responses. This research focused on the quantitative method. Therefore, it is beneficial for data to be collected using other methods in future research. The present study used questionnaire distribution for data collection. It is recommended that future studies use a web-based survey to gather robust data from respondents. The insider threat prevention framework could be expanded to statistically approve the measurement scale for the relationships between other reflective factors and three other constructs in PMT (threat severity, security self-efficacy, and security response efficacy). It is also worthwhile to conduct a comparative analysis between Malaysian organizations and other developed countries such as Singapore and case studies or focus groups to gather rich data concerning the insider threat in organizations.

Acknowledgement

All the papers are retrieved from digital databases, specifically Web of Science, ScienceDirect, and IEEE Xplore. All the work is self-funded.

References

Ahmad, Z., Norhashim, M., Song, O. T., & Hui, L. T. (2016, May). A typology of employees' information security behaviour. In *2016 4th International Conference on Information and Communication Technology*, (pp. 1-4). IEEE. https://doi.org/10.1109/ICoICT.2016.7571929

Alaskar, M., Vodanovich, S., & Shen, K. N. (2015, January). Evolvement of information security research on employees' behavior: a systematic review and future direction. In *2015 48th Hawaii International Conference on*

System Sciences, (pp. 4241-4250). IEEE. https://doi.org/10.1109/HICSS.2015.508

Althebyan, Q., & Panda, B. (2007, June). A knowledge-base model for insider threat prediction. In *2007 IEEE SMC Information Assurance and Security Workshop*, 239-246. IEEE. https://doi.org/10.1109/IAW.2007.381939

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*(3), 613-643. https://doi.org/10.2307/25750694

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, *37*(2), 122-147. https://doi.org/10.1037/0003-066X.37.2.122

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209. https://doi.org/10.1016/j.chb.2016.11.018

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005, June). Towards a theory of insider threat assessment. In *2005 International Conference on Dependable Systems and Networks (DSN'05)*, (pp. 108-117). IEEE. https://doi.org/10.1109/DSN.2005.94

Clubb, A. C., & Hinkle, J. C. (2015). Protection motivation theory as a theoretical framework for understanding the use of protective measures. *Criminal Justice Studies*, *28*(3), 336-355. https://doi.org/10.1080/1478601X.2015.1050590

Crossler, R. E. (2010, January). Protection motivation theory: Understanding determinants to backing up personal data. In *2010 43rd Hawaii International Conference on System Sciences*, (pp. 1-10). IEEE. https://doi.org/10.1109/HICSS.2010.311

Fawzi, H., Tabuada, P., & Diggavi, S. (2014). Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Transactions on Automatic Control*, *59*(6), 1454-1467. https://doi.org/10.1109/TAC.2014.2303233

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, *30*(2), 407-429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Gundu, T., & Flowerday, S. V. (2013). Ignorance to awareness: Towards an information security awareness process. *SAIEE Africa Research Journal*, *104*(2), 69-79. https://doi.org/10.23919/SAIEE.2013.8531867

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*, 106-125. https://doi.org/10.1057/ejis.2009.6

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. https://doi.org/10.1016/j.cose.2011.10.007

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, *34*(3), 549-566. https://doi.org/10.2307/25750691

Junglas, I. A., & Watson, R. T. (2008). Location-based services. *Communications of the ACM*, *51*(3), 65-69. https://doi.org/10.1145/1325555.1325568

Lacey, D. (2010). Understanding and transforming organizational security culture. *Information Management & Computer Security*, *18*(1), 4-13. https://doi.org/10.1108/09685221011035223

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM*, *51*(3), 71-76. https://doi.org/10.1145/1325555.1325569

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, *18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Lee, Y., & Kozar, K. A. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management*, *45*(2), 109-119. https://doi.org/10.1016/j.im.2008.01.002

Legg, P. A., Buckley, O., Goldsmith, M., & Creese, S. (2015, April). Caught in the act of an insider attack: detection and assessment of insider threat. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, (pp. 1-6). IEEE. https://doi.org/10.1109/THS.2015.7446229

Liang, H., & Xue, Y. L. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394-413. https://doi.org/10.17705/1jais.00232

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469-479. https://doi.org/10.1016/0022-

1031(83)90023-9

Magklaras, G., & Furnell, S. (2010). Insider threat specification as a threat mitigation technique. In *Insider Threats in Cyber Security, 49,* 219-244. Boston, MA: Springer US. https://doi.org/10.1007/978-1-4419-7133-3_10

Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. *Information Management & Computer Security*, *14*(4), 361-381. https://doi.org/10.1108/09685220610690826

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431-433. https://doi.org/10.2307/25750685

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health‐related behavior: A meta‐analytic review of protection motivation theory. *Journal of Applied Social Psychology*, *30*(1), 106-143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825. https://doi.org/10.1016/j.dss.2008.11.010

Pahnila, S., Siponen, M., & Mahmood, A. (2007, January). Employees' behavior towards IS security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, (pp. 156b-156b). IEEE. https://doi.org/10.1109/HICSS.2007.206

Park, S., Ahmad, A., & Ruighaver, A. B. (2010, April). Factors influencing the implementation of information systems security strategies in organizations. In *2010 International Conference on Information Science and Applications*, (pp. 1-6). IEEE. https://doi.org/10.1109/ICISA.2010.5480261

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, *67*(2), 1-18. https://doi.org/10.1509/jmkg.67.2.1.18607

Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. (2010). Denial of service attacks in wireless networks: The case of jammers. *IEEE Communications Surveys & Tutorials*, *13*(2), 245-257. https://doi.org/10.1109/SURV.2011.041110.00022

Plotnikoff, R. C., & Higginbotham, N. (2002). Protection motivation theory and exercise behaviour change for the prevention of heart disease in a high-risk, Australian representative community sample of adults. *Psychology, Health & Medicine*, *7*(1), 87-98. https://doi.org/10.1080/13548500120101586

Probst, C. W., & Hansen, R. R. (2009, May). Analysing access control specifications. In *2009 Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering*, 22-33. IEEE. https://doi.org/10.1109/SADFE.2009.13

Randazzo, M. R., Keeney, M., Kowalski, E., Cappelli, D., & Moore, A. (2004). *Insider threat study: Illicit cyber activity in the banking and finance sector, 25,* 1-27. United States Secret Service. *Scribbr.* https://insights.sei.cmu.edu/documents/741/2005_005_001_14420.pdf

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Salleh, N., Hussein, R., Mohamed, N., Karim, N. S. A., Ahlan, A. R., & Aditiawarman, U. (2012). Examining information disclosure behavior on social network sites using protection motivation theory, trust and risk. *Journal of Internet Social Networking & Virtual Communities*, *2012*, 1-11. https://doi.org/10.5171/2012.281869

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2012). Common sense guide to mitigating insider threats *(4th Ed.). Software Engineering Institute, 8-95*. https://doi.org/10.21236/ADA585500

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. In *2006 Innovations in Information Technology*, 1-5. IEEE. https://doi.org/10.1109/INNOVATIONS.2006.301907

Srivastava, P., Singh, S., Pinto, A. A., Verma, S., Chaurasiya, V. K., & Gupta, R. (2011, June). An architecture based on proactive model for security in cloud computing. In *2011 International Conference on Recent Trends in Information Technology (ICRTIT)*, (pp. 661-666). IEEE. https://doi.org/10.1109/ICRTIT.2011.5972392

Tanner Jr, J. F., Hunt, J. B., & Eppright, D. R. (1991). The protection motivation model: A normative model of fear appeals. *Journal of Marketing*, *55*(3), 36-45. https://doi.org/10.1177/002224299105500304

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), 190-198. https://doi.org/10.1016/j.im.2012.04.002

Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, *17*(3), 194-215. https://doi.org/10.17705/1jais.00424

Warkentin, M., Malimage, N., & Malimage, K. (2012). Impact of protection motivation and deterrence on is security policy compliance: a multi-cultural view, *20*, 1-9. *Scribbr.* https://aisel.aisnet.org/wisp2012/20

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, *12(4)*, 324–333. https://doi.org/10.1037/0278-6133.12.4.324

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security, *14*, 367-380. *Scribbr.* https://aisel.aisnet.org/icis2005/31

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*(6), 2799-2816. https://doi.org/10.1016/j.chb.2008.04.005