Ilkogretim Online - Elementary Education Online, Year; Vol 20 (Issue 4): pp. 1118-1126
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.04.123

Relationship between PMT appraisals and Security Practice: Analysis of prevention of insider threat in organization success factor

Rahimah Mohamad Zuwita, Faculty of Art, Computing and Creative Industry, Sultan Idris Education University, TanjungMalim, Perak DarulRidzuan, Malaysia
BahbibiRahmatullah, Faculty of Art, Computing and Creative Industry, Sultan Idris Education University, TanjungMalim, Perak DarulRidzuan, Malaysia

Abstract- Many issues related to insider threat in organization had been debated ever since. Although insider attacks may not occur as frequently as external attacks, they have a higher rate of success, can go undetected, and therefore pose a much greater risk than external adversaries. In relations to that, it is not undeniably the fact that many mechanisms have been proposed in turn to be an initiative to protect data from outside attacks. What worst to comes; those mechanisms could not protect data from authorized users who may misuse their privileges. Due to that circumstances, the development of mechanisms that protect sensitive data from insiders somehow become pitch demand as in method to prevent harm caused by malicious insiders. The purpose of this paper is to find out the relationship between the appraisal process in Protection Motivation Theory (PMT) and security practice. The method of this research is the quantitative method using questionnaire. The findings shows that the contribution of Security Practice towards Perceived Security Vulnerability, Perceived Security Threats, Security Self-Efficacy, Response Efficacy, Prevention Cost, and Maladaptive Rewards. There was positive correlation between all constructs with p< .001. However, the highest relationship is between security practice and maladaptive rewards with 44% of contribution and the lowest relationship is between security practice and response efficacy with 6 % of contribution. Increases in security practice were correlated with increases rating in appraisals processes.

Keywords- Insider threat, Insider attack, Protection Motivation Theory, Organization

I. INTRODUCTION

The traditional notions of cyber security has emphasized on protecting systems or technology against attack that arise from the external threats [1–3] 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 [4,5]. In a recent study by Legg [6], shows that 58% of reported security incidents were as a result of insider threat.

According to 2011 CyberSecurity Watch Survey[(7)], 58% of cyber-attacks on organizations are attributed to outside threats, 21% of attacks are initiated by their own employees or trusted third parties. In addition, as mentioned (8), a lot of incidents were actually are planned in advance. This included individuals which had already involved in the incident and/or potential beneficiaries of the [(9)]insider activity (74%), co-workers (22%), friends (13%), and family members (9%).

Many organizations fail to detect the presence of an insider threat which can cost billions of pounds per year and cause serious damage to the organization, much of which therefore goes unreported and so the true extend 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' to be 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 rate of success, can go undetected, and therefore pose a much greater risk than external adversaries [(10,11)].

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. Infosecurity Magazine has reported that, globally, IS expenditures have reached $55 billion, and it projects that, in 2016, the security expenditure around the world will reach up to $86 billion[(12)].

II. THEORETICAL BACKGROUND

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, behavioral, and economic controls to prevent and deter threats arising from internal and external sources which may originate from human or non-human sources [(13)]. 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 they may be volitional but not malicious [(13)].

Theory is fundamental to research for without it, research does not really exist. Based on literature, few theories have been used relating to insider threat. There are many theories proposed by scholars which came from facets of areas. Meanwhile, significant to this research, behavioral theories such as Theory of Reasoned Action, General Deterrence Theory, Protection Motivation Theory, and such has been identified and as stated by [(14)], these theories explained how behaviors are shaped.

Moreover there are arguments between researchers indicates that technology alone is insufficient to ensure security and have started to pay attention to the human aspect of security[(15–17)]. However as stated by[(18)], knowledge about user security behaviours is far from complete.In addition, perceived susceptibility and severity has been studied by IT security research with inconsistent results. The fact reveal that perceived vulnerability (susceptibility) does not predict whether individuals will execute network security (in their home) but perceived severity does [(16)]. Meanwhile according to [(15)], perceived susceptibility affects users' email security behaviour, but perceived severity does not. On the other hand, [(17)]stated that perceived vulnerability and severity both have an effect on user IT security behavior [(18)].

Furthermore, a more creative research approaches needed in order to retrieve facts on understanding the cognitive and affective processes of both term "white hat" and "black hat" IS security policy violators [20]. The suggest of present study is concerning the term "white hat" (employee, student, contractor, agent, customer) who is projected by organization to indulge with numerous IT security policies and procedures, including devoting in protective behavior such as make a backup of important data, avoiding suspect emails, encrypting mobile data and other activities[(20)].

In addition, malicious IT could be as an agent that continuously invading systems which cause malevolent changes [(18)]. To be added with, based on prior research conducted by [(21–23)], people tend to consider a safeguarding measure by considering how it effectively counters the IT threat, concerning on costs they about to engage, and how convinced they feel about using it[(18)]. Furthermore, as stated by Technology Threat Avoidance Theory (TTAT), emotional disturbance experienced by users often triggered by the perilous prospect of the threat when the threat level is high. This situation automatically generates a problem-focused coping in order to cope the objective threat, as well as utilizing emotion-focused coping to mitigate user's emotional uneasiness [(18)]. Moreover, various form of malicious IT has been continuously jeopardizing the security of contemporary computing environments. To be added with, theory-based empirical research address that computer users' voluntary IT threat avoidance behavior is lacking. This is supported by the fact that most existing security research on individual behavior is focused on organizational settings whereby threat avoidance behavior is mandatory[(18)].

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. However, its importance and influence has also been proven in information security compliance behaviour in recent years. The integration of theory of planned behaviour (TPB) with protection motivation theory (PMT) inspected by [25]to understand information security policies compliance. Overall, his results derived from the business managers and IS professional suggested a great influence of PMT over TPB. Moreover,[26,27]also investigated the integration of protection motivation theory (PMT), 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. PMT has been implied to better understand on what motivates individuals to comply with security policy(24,27), backup data (28,29), as well as employing antimalware software (30,31). This theory also has been adapted to explain various behaviors aimed at protecting home computers and networks (16,32,33) and to explain why users who know how to protect their systems fail to do so (34)However, even though PMT has been applied in InfoSec research, results have been unpredictable and inconsistent(35).

The basic idea of PMT is to have people engage in adaptive actions when dealing with (environmental) risks through perceived risk vulnerability on one hand, and on other hand by considering the possibilities to cope these risks through response efficacy and self-efficacy(36). In threat appraisal process, it involves user on deciding whether he perceives that he is vulnerable to a given threat (perceived vulnerability) and the severity of the threat (perceived severity). The coping appraisal process comprises the user determining whether a protective action is effective at providing protection from the threat (response efficacy), whether he is capable of performing the protective action (self-efficacy) and if it is worth the perceived cost of doing so (perceived cost) (33). In general, increment in threat severity, threat vulnerability, response efficacy and self-efficacy helped adaptive intentions or behaviors. On the other hand, decrement in maladaptive response rewards and adaptive response costs increased adaptive intentions or behaviors. This held true whether the measures were based on intentions or behaviors, and suggests that PMT components may be useful for individual and community interventions (37).

Perceived vulnerability reflects an individual's perceptions of their susceptibility to the harms (36,38–40). Moreover, vulnerability refers to conditional probability the threatening event will occur that no adaptive behaviour is performed or there is no modification of an existing behavioural disposition. Moreover, the perception of vulnerability relates to a person's assessment of his or her probability of being exposed to bad threat. Hence, the probability of adopting the adaptive behaviour increases when a person notices vulnerability as higher(41).Also, being engaged in work activities make employees spend nearly half of their waking lives thus become attached to their organizations, including the organization's goals and stakeholders (e.g., (42)). A positive connection between employees and organizations usually leads to an increase frequency of beneficial activities performed by employees on behalf of their organizations (43,44). Therefore this lead on why many insider feel responsible for protecting organizational information resources from security threats (45). Hence, threat vulnerability should be major component in threat appraisal as well as overall formation of insider's protection motivation(39). In addition, perceived vulnerability is regularly hypothesized to have positive relationship with security practices (33). It is found that a field study of 218 faculty member working at U.S public universities discloses that threat appraisals have a stronger influence on the adoption of anti-plagiarisms software than do coping appraisals (41). In one study, perceived vulnerability was shown to positively influenced intentions to adopt anti-malware software (40). However, it is found that this relationship only held for IS experts and employees in IT intensive industries. Perceived vulnerability did not find a significant relationship with security attitude when explaining whether people will comply with security policies (27). To be added with, a further study did not find a significant relationship between perceived vulnerability and properly securing wireless networks (16). Though, even with the mixed findings from prior research, with the theoretical support from PMT, it is expected that perceived vulnerability will positively influence individuals' security practices (33).

Maladaptive behavior occurs when participants use neutralization techniques (e.g., denial) in order to justify their inappropriate security behaviors (46). Maladaptive rewards is an internal mechanisms for behavioral justification, however they could be rising externally (i.e., extrinsic rewards). Also, in a context of security study,

one can consider that immoral actors may be agreeable to pay an insider for failing to protect the system or for proactively rendering the system more vulnerable (e.g., sharing login information or selling valuable information) (47). Maladaptive rewards can be intrinsic or extrinsic(39). In addition, a previous research has states [101], maladaptive rewards and response costs have influence on the development of protection motivation and also continue to be examined rarely(39). According to PMT, the insider is able to evaluate the security via the threat appraisal process after an insider acquires security threat information (39).

Prevention cost also considered as coping appraisal, which is the cost of performing the recommended behavior. People might refuse from being involved in recommended behaviors when the cost of preventative behaviors is high(38). The perceived costs signify all perceived costs which connected to protective measures or actions, including monetary costs and non-monetary costs such as effort, time, or inconvenience (36). In PMT, they postulates that as the response cost goes up, the probability of performing the adaptive coping response goes down (40). Furthermore, IS research has found support for these findings whereby the intentions of executives to adopt anti-malware software being lower as the response cost is high (40). Nonetheless, these findings reflect regardless of IS expertise or IT intensiveness of an industry the executive works. In addition, further research supports this with the fact that response cost negatively influencing whether people properly secure their wireless network (16). This is supported by other security where a security countermeasure will not occur when the cost of responding to a security threat is greater than the damage of the resulting threat (Lee et al. 2002). In other technology adoption literature, similarly shows that as the cost of using technology increases, an individual becomes less likely to use the technology (48). Such findings from previous research suggest that as the cost of invoking a coping response increases, then the likelihood of implementing the response goes down. Following this, it is expected that response cost will be negatively related to performing security tasks (33).

An emotional response to a threat that expresses, or at least implies, some sort of danger is called fear. Fear has a significant effect on behavior, which lead them to seek ways of removing or coping with the threat and the danger, for most people(49). An appeal communication that involving fear usually attempts to influence or persuade through the threat of impending danger or harm(50). According to (37), fear arousing communications have a significant impact on the selection of behaviors. The fear appeals has been an influence on motivation and this has been widely studied(51). Fear appeals often engage a cognitive processing model(e.g., (52)) even though results were unclear (Peters et al., 2013). According to these process, individuals process their reactions in one of two ways (or in both ways simultaneously, with stronger of two dominating the response). The processes are “danger control” and “fear control” (53). As describe in theories of stress and coping (i.e., (54)) the danger control process shares features with the major cognitive appraisal process. The major cognitive appraisal is essentially an appraisal of threat vulnerability, which individuals engage when confronted with a stressful situation, and the motivation to consider the threat further hinges on their perception of existential vulnerability (54). Also, because of the complimentary positive coping response, PMT predicts that individuals who emphasis on controlling danger are more motivated to deal with the cause of the danger, a given threat is seen as relevant to a person and generates fear that acts as a motivator, not a de-motivator (47).

It is therefore assumed that protection motivation as a countermeasure to security risks in institutions in Malaysia can bring employees closer to information security policies compliance. Also, considering protection motivation as fundamental motivation can bring positive attitude towards the work ethics and security related tasks (55).

III. DATA COLLECTION

Research approach

This phase of research is concerned with the validity of the constructs themselves. It is important to ensuring the validity of the observed variables and capturing 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" 20%. Further company size 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 literature, collected data was analyzed using regression analysis using SPSS 22.

IV. FINDINGS

In order to use survey-based methodology, a key concern is usually regarding assuring the reliability of the scale. 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 into SPSS AMOS 22. In this analysis, we are going to determine the relationship between the appraisal process and security practice.

Annova analysis between Security Practice and Appraisal Process

A one-way between subjects ANOVA (Table 1) was conducted to compare the effect of security practice to threat appraisals. There was a significant effect on security practice on threat appraisals at p <.05 level for the six conditions [F(4,200)= 89.295, p = .00].

Table 1 Annova analysis between Security Practice and Appraisal Process

Annova					
	Sum of Squares	df	Mean Square	F	Sig.
Regression	357.179	4	89.295	56.468	.000e
Residual	316.265	200	1.581		
Total	673.444	204			

Coefficients analysis between Security Practice and Appraisal Process

The coefficient analysis has been run in order to identify linear regression in predicting security practice from those six factors. In linear regression, coefficients are the values that multiply the predictor values. The sign of each coefficients indicates the direction of the relationship between a predictor variable and the responsible variable. A positive sign indicates that as the predictor variable increases, the response variable also increases (Frost, 2020). The threat appraisals support significantly with p< .01. However, perceived security threats has negative relationship with security practice (shown in Table 2).

Table 2 Coefficients analysis between Security Practice and Appraisal Process

Coefficients							
Model	Unstandardized Coefficients		Standardized Coefficient	t	Sig.	Collinearity Statistics	
	β	Std. Error	Beta			Tolerance	VIF
(Constant)	.414	.978		.423	.673		
maladaptiverew	.716	.065	.591	10.961	.000	.809	1.237

ards							
securityselfefficacy	.622	.119	.367	5.210	.000	.473	2.116
perceivedsecuritythreats	-.789	.211	-1.310	-3.740	.000	.019	52.236
perceivedsecurityvulnerability	2.040	.623	1.132	3.274	.001	.020	50.946

Model Summary and Correlations analysis between Security Practice and Appraisal Process

This analysis is purposely to identify the contribution of Security Practice towards Perceived Security Vulnerability, Perceived Security Threats, Security Self-Efficacy, Response Efficacy, Prevention Cost, and Maladaptive Rewards. There was positive correlation between all constructs with p< .001. However, the highest relationship is between security practice and maladaptive rewards with 44% of contribution and the lowest relationship is between security practice and response efficacy with 6 % of contribution (see Table 3). Increases in security practice were correlated with increases rating in appraisals processes.

Table 3 Correlations analysis between Security Practice and Appraisal Process

Correlations							
Pearson Correlation Security Practice	Security Practice	Perceived Security Vulnerability	Perceived Security Threats	Security Self-Efficacy	Response Efficacy	Prevention Cost	Maladaptive Rewards
	1.000	.307	.293	.479	.252	.332	.662
Sig. (1-tailed) Security Practice		.000	.000	.000	.000	.000	.000
N Security Practice	205	205	205	205	205	205	205

V. CONCLUSION AND FUTURE WORK

A user's security behavior is reflected by range of factors that are both internal and external to an individual(15,17).According to Chenoweth (56), PMT suggests that behavioral intention specifies the degree to which someone is willing to try to perform a behavior such as installing and maintaining anti-spyware software (security practice). The more intense their behavioral intention, the higher the probability an individual will adopt anti-spyware software (security practice) (56). A research by (56) they use maladaptive coping which is defined as coping behaviors (i.e. avoidance, denial, hopelessness) that do not directly manage the threat of becoming infected with spyware. PMT predicts that maladaptive coping will negatively impact behavioral intention. Their result shows perceived vulnerability, perceived severity, response efficacy, and response cost influence behavioral intention to use anti-spyware software as a protective technology. Perceived Security Vulnerability and Perceived Security Threats contribute 9% to security practice, Response Efficacy contribute 6%, and Prevention Cost contribute 10% to security practice. The highest correlation/contribution is the relationship between Maladaptive Reward and Security Pactice which contribute 44%. From this cognitive appraisal, it raises protection motivation, which then suggested to develop an attitude change and intent to adopt a recommended (protective) response. The attitude change is not claimed to result from an emotional state of fear, but rather from protective motivation arising out of the cognitive appraisal process (56). As to support which factor triggered insider threat to attack organizational data, which result shown organizational factor, according to (18), most existing security research on individual behavior is focused on organizational settings where the threat avoidance behavior is mandatory.

Finally, the research closed with future work recommendations which may assist researchers to extend and enhance the findings of this research.This research could assists academic researchers to identify research gaps in information security field, focusing on insider threat, including identifying further research needed in this field. This includes examining factors related in different other Asian country. Therefore, the current research

assists in filling a gap in information security field. This research are focusing on quantitative method. Therefore it may be beneficiary for data to be collected using other methods in future research. The present study are using questionnaire distribution for the purpose of data collection. It is recommended that future studies use a web-based survey to gather robust data from respondents.

Acknowledgement

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

Conflict of interest

The authors have no conflicts of interest to declare.

REFERENCES

1. Fawzi H, Tabuada P, Diggavi S. Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks. IEEE Trans Autom Control. 2014 Jun;59(6):1454–67.
2. Pelechrinis K, Iliofotou M, Krishnamurthy SV. Denial of Service Attacks in Wireless Networks: The Case of Jammers. IEEE Commun Surv Tutor. 2011;13(2):245–57.
3. Probst CW, Hansen RR. Analysing Access Control Specifications. In: 2009 Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering [Internet]. Berkeley, California, USA: IEEE; 2009 [cited 2020 Sep 20]. p. 22–33. Available from: http://ieeexplore.ieee.org/document/5341548/
4. Magklaras G, Furnell S. Insider Threat Specification as a Threat Mitigation Technique. In: Probst CW, Hunker J, Gollmann D, Bishop M, editors. Insider Threats in Cyber Security [Internet]. Boston, MA: Springer US; 2010 [cited 2020 Oct 5]. p. 219–44. (Advances in Information Security; vol. 49). Available from: http://link.springer.com/10.1007/978-1-4419-7133-3_10
5. Magklaras GB, Furnell SM, Brooke PJ. Towards an insider threat prediction specification language. Inf Manag Comput Secur. 2006 Aug;14(4):361–81.
6. Legg PA, Buckley O, Goldsmith M, Creese S. 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) [Internet]. Waltham, MA: IEEE; 2015 [cited 2020 Sep 20]. p. 1–6. Available from: http://ieeexplore.ieee.org/document/7446229/
7. Srivastava P, Singh S, Pinto AA, Verma S, Chaurasiya VK, Gupta R. An architecture based on proactive model for security in cloud computing. In: 2011 International Conference on Recent Trends in Information Technology (ICRTIT) [Internet]. Chennai, India: IEEE; 2011 [cited 2020 Oct 5]. p. 661–6. Available from: http://ieeexplore.ieee.org/document/5972392/
8. Randazzo MR, Keeney M, Kowalski E, Cappelli D, Moore A. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. :36.
9. Silowash G, Cappelli D, Moore A, Trzeciak R, Shimeall TJ, Flynn L. Common Sense Guide to Mitigating Insider Threats 4th Edition: [Internet]. Fort Belvoir, VA: Defense Technical Information Center; 2012 Dec [cited 2020 Nov 23]. Available from: http://www.dtic.mil/docs/citations/ADA585500
10. Althebyan Q, Panda B. A Knowledge-Base Model for Insider Threat Prediction. In: 2007 IEEE SMC Information Assurance and Security Workshop [Internet]. West Point, NY, USA: IEEE; 2007 [cited 2020 Sep 23]. p. 239–46. Available from: http://ieeexplore.ieee.org/document/4267567/
11. Chinchani R, Iyer A, Ngo HQ, Upadhyaya S. Towards a Theory of Insider Threat Assessment. In: 2005 International Conference on Dependable Systems and Networks (DSN'05) [Internet]. Yokohama, Japan: IEEE; 2005 [cited 2020 Sep 20]. p. 108–17. Available from: http://ieeexplore.ieee.org/document/1467785/
12. Alaskar M, Vodanovich S, Shen KN. Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction. In: 2015 48th Hawaii International Conference on System

Sciences [Internet]. HI, USA: IEEE; 2015 [cited 2020 Oct 7]. p. 4241–50. Available from: http://ieeexplore.ieee.org/document/7070327/
13. Warkentin M, Johnston A, Straub D, Temple University, Korea University Business School. Neural Correlates of Protection Motivation for Secure IT Behaviors: An fMRI Examination. J Assoc Inf Syst. 2016 Mar;17(3):194–215.
14. Ahmad Z, Norhashim M, Song OT, Hui LT. A typology of employees' information security behaviour. In: 2016 4th International Conference on Information and Communication Technology (ICoICT) [Internet]. Bandung, Indonesia: IEEE; 2016 [cited 2020 Oct 5]. p. 1–4. Available from: http://ieeexplore.ieee.org/document/7571929/
15. Ng B-Y, Kankanhalli A, Xu Y (Calvin). Studying users' computer security behavior: A health belief perspective. Decis Support Syst. 2009 Mar;46(4):815–25.
16. Woon IMY, Tan GW, Low RT. A Protection Motivation Theory Approach to Home Wireless Security. :14.
17. Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test. Comput Hum Behav. 2008 Sep;24(6):2799–816.
18. Liang H. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. J Assoc Inf Syst. 2010 Jul;11(07):394–413.
19. Mahmood, Siponen, Straub, Rao, Raghu. Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. MIS Q. 2010;34(3):431.
20. Warkentin M, Malimage N, Malimage K. Impact of Protection Motivation and Deterrence on IS Security Policy Compliance: A Multi-Cultural View. :10.
21. Bandura A. Self-efficacy mechanism in human agency. Am Psychol. 1982;37(2):122–47.
22. Maddux JE, Rogers RW. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. J Exp Soc Psychol. 1983 Sep;19(5):469–79.
23. Weinstein ND. Testing four competing theories of health-protective behavior. Health Psychol. 1993 Jul;12(4):324–33.
24. Ifinedo P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Comput Secur. 2012 Feb;31(1):83–95.
25. Siponen M, Pahnila S, Mahmood A. Factors Influencing Protection Motivation and IS Security Policy Compliance. In: 2006 Innovations in Information Technology [Internet]. Dubai, United Arab Emirates: IEEE; 2006 [cited 2020 Oct 5]. p. 1–5. Available from: http://ieeexplore.ieee.org/document/4085422/
26. Vance A, Siponen M, Pahnila S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Inf Manage. 2012 May;49(3–4):190–8.
27. Herath T, Rao HR. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur J Inf Syst. 2009 Apr;18(2):106–25.
28. Crossler RE. Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. In: 2010 43rd Hawaii International Conference on System Sciences [Internet]. Honolulu, Hawaii, USA: IEEE; 2010 [cited 2020 Nov 23]. p. 1–10. Available from: http://ieeexplore.ieee.org/document/5428416/
29. Menard P, Gatlin R, Warkentin M. Threat Protection and Convenience: Antecedents of Cloud-Based Data Backup. J Comput Inf Syst. 2014 Sep;55(1):83–91.
30. Johnston, Warkentin. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Q. 2010;34(3):549.
31. Lee Y, Larsen KR. Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. Eur J Inf Syst. 2009 Apr;18(2):177–87.
32. Anderson, Agarwal. Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. MIS Q. 2010;34(3):613.
33. Crossler R, Bélanger F. An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument. ACM SIGMIS Database DATABASE Adv Inf Syst. 2014 Nov 21;45(4):51–71.
34. Workman M. A test of interventions for security threats from social engineering. Inf Manag Comput Secur. 2008 Nov 21;16(5):463–83.
35. Menard P, Bott GJ, Crossler RE. User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory. J Manag Inf Syst. 2017 Oct 2;34(4):1203–30.
36. Bockarjova M, Steg L. Can Protection Motivation Theory predict pro-environmental behavior? Explaining the adoption of electric vehicles in the Netherlands. Glob Environ Change. 2014 Sep;28:276–88.

37. Floyd DL, Prentice-Dunn S, Rogers RW. A Meta-Analysis of Research on Protection Motivation Theory. J Appl Soc Psychol. 2000 Feb;30(2):407–29.
38. Janmaimool P. Application of Protection Motivation Theory to Investigate Sustainable Waste Management Behaviors. Sustainability. 2017 Jun 22;9(7):1079.
39. Posey C, Roberts TL, Lowry PB. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. J Manag Inf Syst. 2015 Oct 2;32(4):179–214.
40. Kumar PR, Raj PH, Jelciana P. Exploring Data Security Issues and Solutions in Cloud Computing. Procedia Comput Sci. 2018;125:691–7.
41. Lee Y. Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. Decis Support Syst. 2011 Jan;50(2):361–9.
42. Porter LW, Steers RM, Mowday RT, Boulian PV. Organizational commitment, job satisfaction, and turnover among psychiatric technicians. J Appl Psychol. 1974;59(5):603–9.
43. Choi JN. Change-oriented organizational citizenship behavior: effects of work environment characteristics and intervening psychological processes. J Organ Behav. 2007 May;28(4):467–84.
44. Thomas JP, Whitman DS, Viswesvaran C. Employee proactivity in organizations: A comparative meta-analysis of emergent proactive constructs. J Occup Organ Psychol. 2010 Jun 1;83(2):275–300.
45. Albrechtsen E, Hovden J. The information security digital divide between information security managers and users. Comput Secur. 2009 Sep;28(6):476–90.
46. Siponen, Vance. Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. MIS Q. 2010;34(3):487.
47. Burns AJ, Posey C, Roberts TL, Benjamin Lowry P. Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. Comput Hum Behav. 2017 Mar;68:190–209.
48. Wu J-H, Wang S-C. What drives mobile commerce? Inf Manage. 2005 Jul;42(5):719–29.
49. Tanner JF, Hunt JB, Eppright DR. The Protection Motivation Model: A Normative Model of Fear Appeals. J Mark. 1991 Jul;55(3):36–45.
50. Rogers RW. A Protection Motivation Theory of Fear Appeals and Attitude Change1. J Psychol. 1975 Sep;91(1):93–114.
51. Witte K, Allen M. A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Educ Behav. 2000 Oct;27(5):591–615.
52. Witte K. Putting the fear back into fear appeals: The extended parallel process model. Commun Monogr. 1992 Dec;59(4):329–49.
53. Witte K. Fear control and danger control: A test of the extended parallel process model (EPPM). Commun Monogr. 1994 Jun;61(2):113–34.
54. Folkman S, Lazarus RS, Dunkel-Schetter C, DeLongis A, Gruen RJ. Dynamics of a stressful encounter: Cognitive appraisal, coping, and encounter outcomes. J Pers Soc Psychol. 1986;50(5):992–1003.
55. Hina. [No title found]. In: 2016 3rd International Conference on Computer and Information Sciences (ICCOINS). Kuala Lumpur: IEEE; 2016.
56. Hole, Y., &Snehal, P. &Bhaskar, M. (2018). Service marketing and quality strategies. Periodicals of engineering and natural sciences,6 (1), 182-196.
57. Hole, Y., &Snehal, P. &Bhaskar, M. (2019). Porter's five forces model: gives you a competitive advantage. Journal of Advanced Research in Dynamical and Control System, 11 (4), 1436-1448.
58. Chenoweth T, Minch R, Gattiker T. Application of Protection Motivation Theory to Adoption of Protective Technologies. Nd Hawaii Int Conf Syst Sci. 2009;10.
59.Yogesh Hole *et al* 2019 *J. Phys.: Conf. Ser.* **1362** 012121