Research Article

A Study on Protection Motivation Theory and Information Systems Security Policy Compliance

S Rajendran*[1], V M Shenbagaraman[2]
[1]Department of Information Technology, SRM University, India.
[2]School of Management Studies, SRM University, India.
***Corresponding author's E-mail:** rajendran.s@ktr.srmuniv.ac.in

Accepted on: 12-08-2016; **Finalized on:** 30-09-2016.

ABSTRACT

Every organization which uses computing systems for business operations has its own information systems security policies (ISP) for its employees to adhere. Failure to comply with the established ISPs by the employees is a major issue in many organizations. Intentional as well as unintentional violations of ISPs cause enormous damages to the organizations. Researchers have criticized that violation of ISPs among the employees happens due to the lack of proper understanding of ISP and the implications of non-compliance. Researchers and academicians have focused their research on identifying the facts behind ISP violations using novel models based on the Protection Motivation Theory (PMT) and on providing recommendations for enhanced adherence behavior to comply with rules. The main objectives of the research in this direction are to motivate the employees to understand their responsibilities in the workplace and encourage them to adhere to the righteous path, thereby adding more benefits to an organization. This survey article provides insights for the scholars and researchers who are interested in this area of study.

Keywords: Information systems Security Policy-ISP, Protection Motivation Theory-PMT, Compliance.

INTRODUCTION

In the last five decades, a considerable amount of research has been done on the influence of fear on persuasion. A number of theories and models of fear appeals, also known as cognitive mediating processes, have been derived. The objective of each one of these studies has been to understand the influence of fear on persuasion and find ways to apply it on specific set of social issues. A fear appeal is defined as a persuasive message that arouses fear by portraying a personally relevant and substantial threat followed by a description of reasonable actions for deterring the threat[1]. The basis for the above is that fear appeals depend on a threat to an individual's welfare which persuades him towards beneficial actions[2].Protection Motivation Theory (PMT) was first introduced by Rogers[3] to better understand the effects of fear appeals on health-related attitude and behavior. In 1983, he revised it to an extended PMT with emphasis on the cognitive processes of mediating behavioral change. It is also stated that PMT[4] is based on the work of Lazarus[5] and Leventhal[6] resulting in threat and coping appraisal processes.

PMT suggests four factors that influence a person's intentions to safeguard him from any harmful or threatening event. The factors are (i) the severity of the harmful or threatening event(perceived severity), (ii) the likelihood of the event occurring (vulnerability), (iii) the effectiveness of the planned preventive steps (response efficacy) and (iv) the ability of the person in executing the plan to reduce the effect of threatening event (self efficacy). The perceived severity and the vulnerability are used to determine the threat appraisal which indicates the degree of significance of the event. Higher threat appraisal indicates decreased likelihood of maladaptive behavior. The threat appraisal has been applied in many health-related studies. The coping appraisal, which consists of response efficacy and self efficacy, focuses on the adaptive responses. It determines the ability of a person to cope with a threat and take up steps to avoid.

PMT is applied mainly in health-related issues to study the behavior of people involved in smoking, drug abuse and alcoholism. Knowing the importance of PMT, most of the researchers have applied it in various fields. Following are some of the areas, where the PMT was applied and has proved to be effective.

- ✓ Promoting water conservation
- ✓ To study the behaviors related to the prevention of nuclear war
- ✓ The assertive behavior in interpersonal communications
- ✓ The problem of burglary by increasing precautionary measures with PMT
- ✓ Increasing earthquake preparedness.

Also, because of its success, PMT is widely applied to study the health-related behaviors. It is been used as a framework for health education interventions designed to influence health behaviors.

Enhancing healthy life-style, reduced alcoholic use, enhancing diagnostic health behaviors and preventing diseases are some of the studies undertaken by the researchers. Later on, scholars involved in the research of the ISPs, have started applying the PMT in their research. IS Security literatures suggest 91% of the organizations' own employees frequently fail to adhere to ISPs[7]. A number of models, to ensure that employees comply with IS security policies, have been proposed and to mitigate policy violations. The model based on PMT is more useful to explain ISP compliance. Siponen M have proposed an extended PMT to explain employees ISP compliance. The main motive of information security research is to educate the individuals in an organization to engage in more secure behaviors. In due course, PMT has occupied a major position in IS security research areas. It provides a theoretical foundation and helps to motivate individuals to change their security related behaviors to protect themselves and their organization.

PMT is well suited for information security contexts in which end users, employees and consumers require additional motivation to protect their information assets. The intention of this article is to provide an extensive survey of PMT and its advancements in recent years. Hence, the survey provides notable information on PMT.

Protection Motivation Theory (PMT) and its variants with respect to ISP

Due to the widespread use of Protection Motivation Theory (PMT), lot of new models have been proposed by the researchers with respect to ISP compliance in an organization. Hence, the following survey presents the new models based on Protection Motivation Theory.

Siponen M have proposed a model that explains employees' security compliance, extended version of PMT is presented by including two additional factors (stated as preceding factors) such as (i) Visibility belief (ii) Normative belief. Also, the model was tested by collecting the information from 5 companies, and the sample size is N=919. It is also stated that the social pressure within the organization and the employees' awareness about the threats of IS Security have influence on cognitive process of PMT. Based on the study conducted certain facts are identified such as (i) The External IS security visibility also has an impact on cognitive process of PMT (ii) Threat appraisal has a significant effect on intention to comply with IS security policies. (iii) The model shows that the preceding factors have a significant effect on threat appraisal, self-efficacy and response efficacy. Hence some sort of education and campaigns are insisted by the authors to have IS security visibility.

In order to study the employees' behavior towards ISP compliance the authors Pahnila S[9] have proposed a novel theoretical approach.

The study comprised of sample size of (N=245) which was collected from a Finnish company. The researchers have come out with the findings as, (i) The Information quality has a significant effect on actual ISP compliance (ii)Attitude, Habits and Normative beliefs have a significant effect on intention to comply with ISPs (iii) Threat appraisal and facilitating conditions have a significant impact on attitude towards complying with ISP.(iv) Coping appraisal does not have significant effect on attitude towards compliance (v)Sanctions do not have a significant effect on intention to comply with IS security policy whereas the rewards do not have a significant effect on actual ISP compliance. These findings provide a way for better understanding of ISP compliance.

An integrated approach of PMT and Deterrence theory for security policy compliance is applied by Herath. T et and Rao H R[10]. The study comprises of a data set of 312 employees from 78 organizations. The authors have concluded that i) perceptions about the severity of breach, the response efficacy and self-efficacy having positive effect on the attitude towards security policies, ii) response cost negatively influences the favorable attitudes iii) social influence has a significant impact on compliance intentions, iv) resource availability has a significant factor in enhancing self-efficacy, which in turn is a significant predictor of policy compliance and v) organizational commitment plays a dual role by impacting intentions directly as well as promoting a belief that employee actions have an effect on organizations' overall security.

As number of socio-cognitive theories has emerged with respect to employees' failure to comply with ISP, the research done by Anthony Vance[11] has identified that prior studies have not considered the influence of past and automatic behavior on employee decisions to comply. Hence to address this gap, the routinized behavior, habit of an individual is integrated with PMT to study the compliance with ISP. As core component of any research being the data collection phase, the authors have adapted to hypothetical scenario method. The survey is done with respect to 111 Information security experts and information security managers at variety of Finnish organizations using open-ended questionnaire but just obtained only 54 responses. Responses will be less as the data is related to security issues which was already stated by A.G. Kotulic, J.G. Clark[12].

Hence sample size (N=54) constitutes only 49% of the response rate. The study has concluded with the findings such as: a) employees must realize the security threats and their impact on their organization, i.e. the issues and consequences with respect to ISP violation must be explained. b) employees must understand that ISP is a part of their work responsibility. It is also stated that the organizations must ensure that security policies should be easy to follow, so that ISP compliance can be met.

Approaching the problem of ISP with respect to an organization, the researchers Siponen M[13] have introduced a new multi-theory based model that explained employees' adherence to security policies. The model combines the aspects of protection motivation theory, the theory of reasoned action (TRA), and the cognitive evaluation theory. Four corporations in Finland is chosen for data collection and 669 responses are received. The factors such as perceived severity, perceived vulnerability, employee's attitude towards ISP and social norms complying with the policies have been studied. The research has insisted that the high level managers must warn employees to realize the importance of information security. Also security education and hands on training is insisted for the insiders.

A researcher Ifinedo, P[14] has investigated the ISP compliance by integrating theories such as TPB (the theory of planned behavior) and Protection Motivation Theory (PMT). Using the partial least squares(PLS) data analysis is done with sample size of 124 business managers and IS professionals. The study reveals the facts such as (i) self-efficacy (ii) attitude towards compliance (iii) Subjective norms (iv) response efficacy and (v) perceived vulnerability, have positive influence towards ISP whereas the analysis did not support factors such as (i) perceived severity (ii) response cost towards ISP.

Protection Motivation Theory Applications

As PMT sets a strong foundation in the information security field, some of the researchers have applied it to study the various aspects in the organization based on ISP compliance and the following illustrates few of them.

Study of security lapses

The research by Workman M[15] highlights some information on information security contravention behaviors such as security lapses and provides some behavioral recommendations such as ethics training or punishment of offenders. It is stated that because of the careless employees omitting the information security measures in an organization contributes to significant civil losses and even to crimes. Hence, an empirical study is done using PMT and a threat control model (TCM) is used to validate the assumptions for better understanding of the “knowing-doing” gap. A random sample of (N= 588) people were taken from a large technology-oriented services corporation. The summary of the work is given below:

(a) The data collection is done with 2 techniques. (i) On-line questionnaire (ii) Direct observation of behaviors via computer logs. The research addresses “What to educate” question.

(b) A Technique known as benign hacking or white-hat penetration or controlled exploitation has been used to find technological vulnerabilities in security infrastructure.

(c) As threats should not be underestimated, it is expected that the Chief Security officers and other security officials must communicate the actual threat levels to the employees.

(d) In order to reduce security lapses, the behavioral modification simulation software was proven to be a better solution.

(e) The research insists the use of “the right” security technology and expected to be user-centered. Hence, it is also stated that the knowing-doing gap cannot be ignored as it is fundamental to the implementation of security measures.

PMT to Adoption of Protective Technologies

The authors Tim Chenoweth[16] have applied PMT to Adoption of Protective Technologies which tends to avoid destruction from rising number of negative technologies such as malware. The study is done using PMT-based model. The same is tested in the undergraduate student computer users, sample size (N=232).The study reveals that among the core components, the security with respect to self-efficacy, response efficacy have shown positive influence of backing up of data whereas the threat appraisal construct a negative relationship with the behavior though it contradicts the expectations. The authors have concluded that the extensions of research could be exploring more combinations of threats and behaviors, particularly in exploring the use of anti-spyware software for preventing identity theft and the usage of firewalls to avoid file loss.

PMT in Multiple Theoretical Perspectives

The research was undertaken by Anthony Vance[17] to identify the deliberate IS security policy violations by proposing three guidelines. Based on the groundwork undertaken by the researcher, it is stated by the researcher that none of the existing research as of that period were able to meet more than one guideline. Having these guidelines as a base, IS Security policy violations have been analyzed using three models constructed from theories such as : (i) Neutralization theory (ii) Rational choice theory and (iii) Protection Motivation theory. The study was conducted with 1423 professional respondents from 7 organizations across 47 countries and has identified the reasons behind violating the IS policies. Also, the implications for improving IS compliance for the practitioners was suggested.

PMT in Understanding Determinants to Backing up of Data

To understand the Determinants to backing up of personal data, Robert E. Crossler[18] have used PMT. The author has collected data through on-line and paper sources. The survey size is about 112. With respect to that of backing up of data, the author states that computer self-efficacy and response efficacy have a positive effect on the backing up of data, while the perceived security vulnerability and perceived security threat affects the backing of data negatively.

PMT in Tobacco Research

The authors MacDonell K[19] have done a study with respect to the tobacco consumption by applying PMT. A data set comprising of 553 Chinese vocational high school students are accounted. Based on the feedback from students, teachers and researchers, the measurement scale was proposed using PMT for the research purpose. The Measurement scale reflects the structure of PMT and also explains the acceptable reliability with respect to tobacco use. The factors such as intention to smoke and the actual smoking behavior are clearly addressed by the tool.

To be more specific, the acceptability, validity, and reliability issues of PMT scale clearly address the usage of tobacco and health consequences.

Despite the effectiveness of scale, the weakness (the responsiveness must be redefined multiple times) of the tool is discussed to get better results. Hence, through this research work, the authors have created awareness with respect to tobacco consumption limits.

ISP Compliance Related Theories and Guidelines

On realizing the importance of ISP Compliance, various theories and guidelines have evolved. The following discussion is based on the aforesaid aspect.

ISP and Psychological/Social Theories

The authors Myyry[20] have done empirical study to examine the impact of moral reasoning on compliance with information security policies.

They have designed a theoretical model integrating two psychological theories such as (i) The Theory of Cognitive Moral Development by Kohlberg and (ii) Theory of Motivational types by Schwartz.

The empirical findings have shown that the proposed model was supportive and also the implications of the practice and research on how to improve the ISP compliance were stated.

As employees subvert existing ISP, there are chances of large amount of IS incidents. Hence, Cheng L[21] have designed a theoretical model based on both deterrence and social bond theories.

The model is evaluated using the survey of data set comprising of 185 employees belonging to the organizations in Dalian, China.

The results highlight that both informal and formal controls have a better effect on employees' ISP violation intentions.

Also, it is found to be proved that the social pressures exerted by subjective norms and co-worker behaviors have significant influence with respect to ISP violations.

ISP and Systematic Based Taxonomy

It is well stated by the researchers Posey C[22] that, for protecting the organizations' resources one should not solely depend on the technology but also on the employees, the insiders.

Hence based on this aspect the research has set its focus. Semi-structured interviews with 11 information security professionals and 22 ordinary organization insiders (N=33) are carried out.

The study used a six step methodology of qualitative and quantitative approaches. It uses various classification techniques such as (i) MDS, multidimensional scaling (ii) ProFit, property fitting and (iii) Cluster analysis.

The research has given more insight on protection motivation behaviors and serves as a comprehensive guide for the researchers.

ISP Violations and Guidelines

The authors Siponen M. and Vance A[13] have stated that by carefully addressing contextual issues in instrumentation design, IS behavioral research could be improved. Hence, they have formulated 5 guidelines for the researchers, editors, reviewers in the field of ISP which are: (i) ensure that respondents recognize the phenomenon of intent in the instrumentation (ii) measure the phenomenon completely (iii) ensure that the dependent variables focus on the important problem in practice (iv) ensure the applicability of IS security violations to the organizational context (v) theorize the appropriate level of specificity, generalizability for instrumentation.

Enhancing ISP Compliance

Considering the security awareness, Lebek B[23] conducted a review by considering 113 publications and found that 54 theories with respect to employees' ISP. Almost most of the research works depends on the primary theories such as TPB, GDT, PMT and TAM. The literature study identifies the gap and addresses the gap for improving awareness in behavioral research. The research states the importance of development of measures and process models to address the gap between theory and practice.

The authors Sommestad T[24] have identified the significance of the variables which influence compliance with ISP. For the research purpose 29 studies have been attempted and around 60 variables are identified and also stated that the impact of these variables have small contribution towards people's behavior. For decision makers seeking guidance to improve employees' ISP compliance, the problem of dealing with large number of variables whose strength and interplay are uncertain and unknown is quite a challenge. Topa I. and Karyda M[25] identified and categorized critical factors that shape employee security behavior and list security management practices to enhance security compliance. Hence, to enhance security policy compliance 3 courses of actions are suggested by the researchers as (i) addressing the individual issues that hinder compliance (ii) creating a suitable organizational setting: rewards and sanctions (iii) taking into consideration of the technological aspects. To conclude the authors have suggested the need to design user-friendly security tools for ISP Compliance.

Protection Motivation Theory and its variants have played a major role in understanding the protection motivated behaviors of employees and individuals towards ISP compliance and securing his/her data respectively. The Table 1 summarizes the variations in the PMT model for bringing improvements with respect to ISP.

Table 1: Summary on PMT Variations

Author; Journal (J); Year	Research Focus	Variants in the Existing PMT Model	Components of New Model: Other than Core components of PMT
Siponen M, 1-4233-0674-9/06 ©2006 IEEE.	Employees' Information security policy Compliance	Theoretical Model: Extended PMT	Preceding factors (i) Normative beliefs (ii) Visibility
Pahnila S. PACIS 2007 Proceedings. http://aisel.aisnet.org/pacis 2007/73.	Attitude towards compliance, intention to comply and compliance with IS security policies	Theoretical Model: Integrated approach PMT is integrated with other theories	(i) General deterrence theory (ii) Theory of reasoned action (iii) Information systems success (iv) Triandis' Behavioral framework (v) Rewards
Workman et al; Computers in Human Behavior, 24(6), 2008, 2799-2816.	ISP violation among the insiders	Extended PMT called TCM: Threat Control Model is introduced to address "Knowledge-doing gap"	TCM: (i)Threat assessment (ii)Coping assessment
Myyry L. European Journal of Information Systems, 18(2), 2009, 126-139.	Influences of moral reasoning on Compliance with ISP	A Theoretical Model is proposed based on two Psychological theories (i) Theory of Cognitive moral designed by Kohlberg(1969) (ii) Theory of Motivational types of values by Schwartz (1992).	The New model is based on the (i) Moral reasoning (ii) Values
Herath T. and Rao H.R. European Journal of Information Systems, 18(2), 2009, 106-125.	Designing a framework for security policy compliance in organizations.	Integrated approach of PMT and Deterrence theory.	Role of deterrence (i) Punishment and severity (ii) Certainty of detection items
Anthony Vance, Academic dissertation presented with the assent of the Faculty of Science, University of Oulu. (2010)	To study the reason behind the ISP violations among the employees using theories from criminology and psychology.	ISP violations are studied by using different data sets on various theories. i. PMT – Psychology ii. General deterrence theory - Criminology iii. Neuralization theory – Criminology. [The theories are addressed separately].	(i) Setting the guidelines for study of ISP (ii) To study the impact of guidelines with respect to the theories undertaken (iii) To address all the components in PMT. In fact it is also stated that, it is the first study to address all the components of PMT
Anthony Vance, Mikko Siponen, Seppo Pahnil, 2012, 0378-7206/$ ©2012 Elsevier.	To study the improved ISP violations.	Integrated Model is designed with Habits (a routinized behavior) and PMT	The integrated approach has a strong impact with respect to ISP compliance
Ifinedo P., Computers & Security, 31(1), 2012, 83-95.	To study the ISSP violations.	Integrated Model TPB - Theory of Planned Behavior and PMT.	It is stated that ISP compliance has positive effect on self-efficacy, response efficacy, and attitude towards compliance, perceived vulnerability and subjective norms.

CONCLUSION

Research has made known that Protection Motivation Theory could be applied in health related areas, successfully.

PMT has been applied in various studies related to cancer prevention, tobacco usage, addiction to alcohol, AIDS prevention, observance of medical prescriptions, and topics related to personal health. PMT was also used in studying students' intentions to attend classes regularly and in reducing malpractices in examinations. Non-adherence to organizations' stated policies is a major problem. Studies have shown how a unified PMT could be used to determine the steps taken by individual home users to their systems from malware and the security training required for them. In a digitized world, where information is everything, not following the information systems security policies leads to loss of business, reputation and legal issues.

Researchers have used PMT combined with other social theory models and suggested guidelines for improved compliance of ISPs.

There is scope for further research in this area. Research may be conducted to find whether there is change in Protection Motivation Behavior (PMB) with change in cultures.

Scholars can also explore how the PMBs of Gen-Y (Millennials) would differ from that of Gen-X and baby boomer generations towards ISP compliance.

To the best our knowledge, there are not many published articles from Indian researchers focusing on applying social, psychological and criminological theories to information security field.

Hence it is expected that this article would motivate the scholars to focus on this area.

REFERENCES

1. Kim Witte. Message and Conceptual Confounds in Fear Appeals: The Role of Threat, Fear, and Efficacy. The Southern Communication Journal, 58(2), 1993, 147-156.
2. Gore P., Madhavan S., Curry D., McClurg G. Persuasive Messages. Marketing Health Services, 18(4), 1998, 32-43.
3. Rogers R. W. A protection motivation theory of fear appeals and attitude change. Journal of Psychology, 91(1), 1975, 93-114.
4. Rogers R. W. Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology: A source book, New York, NY: Guilford Press, 1983, 153-176.
5. Lazarus R.S, "Psychological stress and coping process", Newyork: McGraw Hill, 1996.
6. Leventhal H. "Findings and theory in the study of fear Communications". In L. Berkowrtz (ed) Advances in Experimental social psychology, New York, Academic Press, Vol.5, 1970, 119-186.
7. Hinde S. Security surveys spring crop. Computers & Security, 21(4), 2002, 310-321.
8. Siponen M, Pahnila S, Mahmood A. Factors influencing protection motivation and IS security policy compliance. In 2006 Innovations in Information Technology 2006 Nov (pp. 1-5). IEEE.
9. Pahnila S., Siponen M. and Mahmood A. Employees' behavior towards IS security policy compliance. In System sciences, 2007.HICSS 2007. 40th annual hawaii international conference on IEEE, 2007, January, 156b-156b.
10. Herath T. and Rao H.R. "Protection motivation and deterrence: a framework for security policy compliance in organizations". European Journal of Information Systems, 18(2), 2009, 106-125.
11. Anthony Vance, MikkoSiponen, Seppo Pahnil. "Motivating IS Security Compliance: Insights from Habit and Protection Motivation theory", 0378-7206/$ ©2012 Elesevie.
12. A.G Kotulic, J.G. Clark. Why there aren't more information security research studies, information and management 41(5), 2004, 597-607.
13. Siponen M. and Vance A. "Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations", European Journal of Information Systems, 23(3), 2014, 289-305.
14. Ifinedo P. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory." Computers& Security, 31(1), 2012, 83-95.
15. Workman M., Bommer W.H. and Straub D. "Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior", 24(6), 2008, 2799-2816.
16. Tim Chenoweth, Robert Minch, Tom Gattker. "Application of Protection Motivation Theory to Adoption of Protective Technologies", 978-0-7695-3450-3/09 ©2009 IEEE, 2009.
17. Anthony Vance, "Why do Employees violate IS security policies: Insights from Multiple Theoretical Perspectives", Academic dissertation presented with the assent of the Faculty of Science, University of Oulu 2010.
18. Robert E. Crossler, "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data", Proceedings of the 43rd Hawaii International Conference on System Sciences, 978-0-7695-3869-3/10 IEEE 2010.
19. MacDonell K, Chen X, Yan Y, Li F, Gong J. A Protection Motivation Theory-Based Scale for Tobacco Research among Chinese Youth, Journal of Addiction & Therapy, Volume 4: issue 3: 154. doi:10.4172/2155-6105.1000154, 2013.
20. Myyry L, Siponen M., Pahnila S., Vartiainen T., & Vance A. "What levels of moral reasoning and values explain adherence to information security rules & quest: an empirical study", European Journal of Information Systems, 18(2), 2009, 126-139.
21. Cheng L., Li Y., Li W., Holm E. and Zhai Q. "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory". Computers & Security, 39, 2013, 447-459.
22. Posey C., Roberts T., Lowry P.B., Bennett B. and Courtney J. "Insiders' protection of organizational information assets: Development of a systematic - based taxonomy and theory of diversity for protection-motivated behaviors". Mis Quarterly, 37(4), 2013, 1189-1210.
23. Lebek B., Uffen J., Breitner M.H., Neumann M. and Hohler B. January."Employees' information security awareness and behavior: A literature review", In System Sciences (HICSS), 2013 46th Hawaii International Conference on IEEE. 2013, 2978-2987.
24. Sommestad T., Hallberg J., Lundholm K. and Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Information Management & Computer Security, 22(1), 2014, 42-75.
25. Topa I. and Karyda M. "Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance" In Trust, Privacy and Security in Digital Business, Springer International Publishing Switzerland, 2015, 169-179.

Source of Support: Nil, **Conflict of Interest:** None.