pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220980

Personality Traits and Security Motivation

Arnstein VESTAD[a,1]
[a] *NTNU – Norwegian University of Science and Technology, Trondheim, Norway*

Abstract. *Security awareness training has long been considered a critical element in organizational cybersecurity preparedness and a mandatory activity in many laws and regulations as well as cybersecurity management standards such as ISO 27001. Organizations approach the issue with different methods, but many rely on online training as a cost-effective way to reach a large number of employees at a low cost. When this training is delivered as a voluntary measure, it is essential to have knowledge about the factors contributing to motivation to participate. This study uses the theoretical concepts from Protection motivation theory (PMT) as well as looking into how individual personality traits might affect the willingness to participate. A survey was conducted in a large Norwegian municipality and the data analyzed with PLS-SEM. The study found support for the concepts of Cost and Effectiveness affecting Motivation, but not Vulnerability and Severity. The personality traits of Extroversion and Agreeableness was found to have some moderating effect*

Keywords. Security awareness, protection motivation theory, personality traits

Introduction

The human element of cyber security has long been a focus of research [1] and according to the 2021 Verizon data breach report[2] 85% of breaches involved a human element and 36% of all breaches involved phishing. For this reason, user education and awareness is seen as a crucial element of cyber security programs in organizations, also demonstrated by its inclusion in many security management standards, such as ISO 27001. In the health care sector, where frontline workers continually manage highly sensitive information while under continuous pressure of medical emergencies and other stressful situations, the human aspects of cybersecurity come to the frontline. Security awareness training in organizations ranges from simple education on security policies (password strength and reuse, rules for sharing of information etc.) to more complex themes such as increased understanding of threat actors, how to spot phishing emails or understanding privacy concepts such as personally identifiable information (PII) that are critical to the security of organizations. In line with the increased digitalization of health care services, awareness training methods have also moved from classroom/lecture-based or distribution of written policies to more interactive digital solutions, increasing the possibility of adapting the training to personal preferences and learning styles.

Research has highlighted the problem of employee motivation toward security awareness programs and the need for a better understanding of how employees perceive

[1] Corresponding Author, Arnstein Vestad, Department of information security and communication technology, NTNU, Norway; E-mail: arnstein.vestad@ntnu.no.

such training[3]. While there have been many studies of security awareness, awareness training and its effects on security compliance and security behavior in organizations, see [1] for a review, few have looked into how personality traits affect attitudes to security compliance or actual behavior. While [4] considered personality effects on security compliance and [5] on risk-taking behavior, the present study focuses on motivation and addresses this by using a survey that combines concepts from the security awareness literature and scales for the measurement of personality traits, as well as participation in voluntary security awareness training.

A large municipality in Norway with interest in the success of their security awareness training activities was selected as the case for this study. The municipality has conducted semi-yearly security awareness campaigns. The training has so far been conducted voluntarily and this presented an interesting opportunity to investigate factors contributing to motivation and how traits contribute to motivation and participation that would not be possible in a mandatory setting.

From a research perspective this study contributes to better theories and understanding of how individual psychological traits affect cybersecurity behavior. From a practical perspective, the research can contribute to better awareness training systems by adopting the training to individual parameters, thus supporting better training outcomes. In the study, a questionnaire was constructed based on theories of security awareness and protection motivation theory, as well as a short-form personality scoring scale, and the results were analyzed quantitatively with PLS-SEM.

1. Theoretical background

1.1. Security awareness training

The authors of [3] describe several challenges with security awareness training in organizations, such as the gap between the understanding of security professionals and ordinary employees, the need to adapt to the receiver's knowledge level, advice fatigue where employees fail to adapt to security requirements due to the stressful nature of the amount of advice, policies and requirements, the employee's perception of the advice as superficial and unsystematic, or the monotonous nature of the training programs.

1.2. Theories of protective behavior

Many theoretical frameworks have been applied to the study of security awareness in organizations, or more specifically, how attitudes and beliefs contribute to security behavior, for example compliance with security policies. The authors of [1] identified four major theories most frequently used in studies that all try to explain either behavioral intention or actual behavior, Theory of reasoned action/theory of planned behavior (TRA/TPB), General deterrence Theory (GTR), Protection Motivation Theory (PTM) and Technology acceptance model (TAM). (TRA/TPB), developed by Aizen [6] seeks to explain intention and behavior by *attitudes*, *subjective norms* and *perceived behavioral control*. GTR [7] rooted in criminology, focus on the individual's choice not to commit a crime by evaluating the risk of sanctions. In PMT [8] the individual's "protection motivation" – understood as the intention to perform some protective behavior (for example, stop smoking) is calculated based on a threat appraisal taking into account the perception of severity and one's vulnerability to a threat, and a coping appraisal taking into account ones perception of how effective the response will be and how likely one is to succeed. Lastly, in TAM [9], behavior (specifically the adoption of technology) is influenced by the perceived usefulness and ease of use.

The protection motivation theory (PMT) concepts were considered the most relevant for this study. The studied behavior is voluntary, and GTR is more appropriate in a non-voluntary context. TRA/TPB and TAM are more generic models less concerned with threat evaluation as a driving factor in security assessment and choices concerning cybersecurity behavior. PMT has been applied in many studies in information systems research with sometimes inconsistent findings, but the authors of [10] have conducted a meta-analytic study of 92 published studies utilizing PMT. Their findings suggested that the PMT relationships are stronger in a personal context but that the intention-behavior relationship was most robust in a workplace relationship. Their study also found good support for response- and self-efficacy, but no support for response cost.

In our study, we choose to keep all variables from PMT theory to contribute to data for the general model – except for self-efficacy. Self-efficacy is generally in PMT understood as the individual's evaluation of their ability to perform the protective behavior – in this instance, the behavior is rather simplistic – participating in online training – for this reason, we consider self-efficacy in this specific context less relevant.

1.3. Personality traits

The Five-Factor Model of personality traits is the leading framework for theorizing around psychological traits of personality, understood as cross-situationally consistent and relatively enduring patterns of thoughts, feelings and actions [11]. The FFM consists of the five dimensions Extraversion (E), Agreeableness (A), Conscientiousness (C), Neuroticism (N) and Openness to Experience (O). As these traits signify consistent thought patterns, it is reasonable to assume they will also affect decisions concerning individual cybersecurity behavior.

For example, [12] studied the effect of personality traits on the adoption of security tools. The study found that Conscientiousness and Agreeableness moderate the relationship between behavioral intent and extent of use, conscientiousness was found to have a moderate moderating impact, and Agreeableness had a small to medium moderating effect.

In [13], the moderating effect of personality on factors influencing the intention to violate security policies in organizations was studied. The study combined the threat and coping appraisal from protection motivation theory with deterrence theory, where a person is deterred from performing policy violations by the threat of sanctions (severity and likelihood of receiving the sanction). They found that more agreeable persons would be more affected by their evaluation of self-efficacy, that is, their ability to adhere to the policies, more conscientious persons would be more affected by their evaluation of the severity and possibility of sanctions. In contrast, the more neurotic persons were most affected by their evaluation of the Cost of performing the correct behavior.

The FFM is traditionally measured using extensive questionnaires, the most comprehensive being the 240-item NEO Personality Inventory, Revised (NEO-PI-R), but shorter versions have been developed - in this survey the ten-item TIPI scale of [14] was used – comprising only ten questions the personality scale takes only 1 minute. The individually validated Norwegian translation of TIPI was used [15].

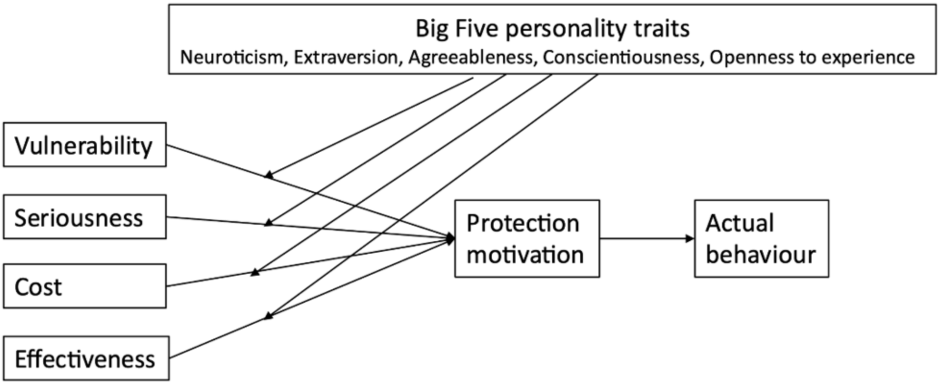
Big Five personality traits
Neuroticism, Extraversion, Agreeableness, Conscientiousness, Openness to experience
Vulnerability
Seriousness
Cost
Effectiveness
Protection motivation
Actual behaviour

Figure 1- Research model and hypothesizes

2. Methodology

A questionnaire was developed based on the theoretical concepts from PMT to reflect the concepts of *Perception of vulnerability*, *Perception of seriousness*, *Response effectiveness*, *Cost*, and *Protection motivation* when it comes to participating in online security training. In addition, the TIPI scale was included to give a measure of personality for the respondents. A pilot of the questionnaire was performed with a subset of respondents (excluded from the final survey) to validate language and scales. An overview of the research model is presented in figure 1.

The questionnaire was distributed to two groups of employees – group A was selected from employees that had chosen to participate in the voluntary awareness training, and group B from employees that had chosen to abstain – this allowed the combination of actual participation in the training with the questionnaire responses while maintaining full anonymity for the participants. Responses were collected through the service Nettskjema.no, configured not to collect personally identifiable information.

3. Findings

Of the 1500 respondents invited to participate, a total of 126 responses were received, giving a total response rate of 8,4%. For group A (500 invited), 115 responded, with a rate of 23%, for group B (1000 invited), 11 responded, with a rate of 1,1%. While the response rate was low, the total number of respondents are sufficient for the ten-power criterion for using PLS-SEM (a sample number a minimum of ten times the number of in-going relations to the endogenous variable). To verify internal validity and composite reliability, Cronbach's alpha, Rho_A, composite reliability and Average variance extracted were calculated for the PMT concepts. Composite reliability and Cronbach's alpha for all constructs were over 0.7, and AVE as a measure for convergent validity is greater than 0.5 as recommended by the literature. A bootstrapping with 5000 samples was then conducted in SmartPLS to establish p-values for the relationships to check of significance of the relationships

Of the relationships investigated from the PMT theory, only Cost and Effectiveness was found to be significant with a p-value < 0.05. Of these Effectiveness had a 0.5

positive effect while Cost had a -0.33 negative effect. From the personality moderation effects, the moderating effect of Agreeableness on Cost (effect 0.13) and Extraversion on Effectiveness (-0,18) was found significant. All other relationships were not found to be significant. For the model in total, the included variables gave a R-score of 0.827 signifying that the included variables contributed to 83% of the variance in Motivation.

A multi-group analysis was planned to investigate difference between participants and non-participants. Due to the low sample size, it was impossible to perform this analysis on the full model. In an analysis on just Cost and Effect no significant group difference was found (likely due to the low sample size for non-participants).

4. Discussion

The data analysis did not support the evaluation of Seriousness and Vulnerability as motivating factors for participation. While this differs from other studies utilizing PMT, it is in line with other studies finding that the coping appraisal (Cost, effectiveness) have stronger effect than fear appraisal (seriousness, vulnerability). The coping appraisal process has much in common with other technology acceptance models where effectiveness and usability play a greater role, such as the technology acceptance model (TAM) [7]. The reason may be that the respondents do not see security awareness training as a direct protective measure, but consider participation more abstractly focusing on utility and Cost (is it useful, do I have time…).

The significant moderating relationship of Agreeableness on Cost signifies that respondents with a higher score on Agreeableness is less likely to let evaluation on Cost affect Motivation. In [9] agreeableness is described by "forgiving attitudes, belief in cooperation, inoffensive language, reputation as a pushover". This may be interpreted as respondents with a higher belief in cooperation being more likely to accept and participate in voluntary training measures, trusting the organizations evaluation of the value of the measure than their own evaluation. The significant negative moderating effect of Extraversion on Effectiveness signifies that respondents with a higher score on Extraversion are less likely to let their evaluation of the measure's effectiveness contribute to their motivation to participate. In [9] extraversion is described by "social skills, numerous friendships, enterprising vocational interests, participation in sports, club memberships". This may be interpreted as the respondents placing higher value on external valuations of usefulness, such as managers and peers, than own evaluations.

While there is some evidence from the analysis to assume that personality does have a moderating effect on participation in voluntary awareness training, the relationships are not large, with effects of 0,13 and -0,18. Caution is therefore advised to when it comes to placing too much reliance on the use of personality measures in the design of and recruitment to voluntary measures. While the concepts of Severity and Vulnerability have been found significant in other PMT-based studies [8], they seem to have less effect in relation to more abstract concepts such as security awareness training in general. The significant difference in response rate for participants and non-participants is also notable. While the direct reasons was not studied directly, in practice, this might signify that email-based awareness training is not the optimal way of reaching or motivating a large proportion of the organization's employees, especially for employees who are not typical office workers, such as in the health care sector. While inexpensive, the effectiveness is questionable when large groups of employees do not participate. Further studies of how to reach these groups should be performed, for example, through qualitative interviews with non-participants. The current study also has other limitations, for example, other important factors such as individual differences in stress levels, age, sex, and cultural differences were not considered.

5. Conclusion

Our findings suggest that participation in online security training is affected more by pragmatic usefulness/usability evaluations than by threat evaluations, so further studies should focus on methods to improve actual and perceived usefulness and ease of use. From a practical perspective, employing organizational social pressure to participate, and focusing on the personal advantages of the training can also be suggested to improve participation.

Acknowledgements

This work has received funding from the Research Council of Norway through the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS) project no. 310105

References

[1] Lebek B, Uffen J, Neumann M *et al.* Information security awareness and behavior: a theory-based literature review. *Management Research Review* 2014;**37**:1049–92.

[2] 2021 Data Breach Investigations Report. *Verizon Business*.

[3] Reeves A, Calic D, Delfabbro P. "Get a red-hot poker and open up my eyes, it's so boring" 1: Employee perceptions of cybersecurity training. *Computers & Security* 2021;**106**:102281.

[4] Johnston AC, Warkentin M, McBride M *et al.* Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems* 2016;**25**:231–51.

[5] McCormac A, Zwaans T, Parsons K *et al.* Individual differences and Information Security Awareness. *Computers in Human Behavior* 2017;**69**:151–6.

[6] Ajzen I. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 1991;**50**:179–211.

[7] D'Arcy J, Herath T. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur J Inf Syst* 2011;**20**:643–58.

[8] Maddux JE, Rogers RW. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology* 1983;**19**:469–79.

[9] Davis FD, Bagozzi RP, Warshaw PR. User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science* 1989;**35**:982–1003.

[10] Mou J, Cohen J, Bhattacherjee A *et al.* A Test of Protection Motivation Theory in the Information Security Literature: A Meta-Analytic Structural Equation Modeling Approach. *JAIS Preprints (Forthcoming)* 2022.

[11] Costa P, McCrae RR. A five-factor theory of personality. *The Five-Factor Model of Personality: Theoretical Perspectives* 1999;**2**:51–87.

[12] Shropshire J, Warkentin M, Sharma S. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security* 2015;**49**:177–91.

[13] Warkentin M, McBride M, Carter L *et al.* The Role of Individual Characteristics on Insider Abuse Intentions. *AMCIS 2012 Proceedings* 2012.

[14] Gosling SD, Rentfrow PJ, Swann WB. A very brief measure of the Big-Five personality domains. *Journal of Research in Personality* 2003;**37**:504–28.

[15] Thørrisen MM, Sadeghi T, Wiers-Jenssen J. Internal Consistency and Structural Validity of the Norwegian Translation of the Ten-Item Personality Inventory. *Frontiers in Psychology* 2021;**12**.