Jan 17th, 12:00 AM

The Role of Situational Risk Propensity in Technology Threat Avoidance Behavior

Tizian Matschak
University of Goettingen, Germany, tizian.matschak@uni-goettingen.de

Theresa Pfaff
University of Goettingen, Germany, theresa.pfaff@stud.uni-goettingen.de

The Role of Situational Risk Propensity in Technology Threat Avoidance Behavior

Tizian Matschak[1], Theresa Pfaff[1]

[1] University of Goettingen, Goettingen, Germany
{tizian.matschak, theresa.pfaff }@uni-goettingen.de

Abstract. The effectiveness of organizational security solutions is affected by individuals' awareness about technology threats. The technology threat avoidance theory (TTAT) has served as a theoretical lens to understand the relationship between technology threats and individual threat avoidance behavior. Recent research has suggested that an individual's dispositional risk propensity can influence the perception of technology threats in TTAT. However, there is a lack of knowledge on how situational risk propensity influences the motivation and behavior toward avoiding technology threats. Our research in progress aims to investigate the impact of situational risk propensity on the perception of technology threats. We argue that situational risk propensity can impact the awareness of technology threats and therefore influence technology threat avoidance behavior. This research in progress enriches existing literature by integrating situational risk propensity in TTAT.

Keywords: Cybersecurity, Situational Risk Propensity, Technology Threat Avoidance Theory.

1 Introduction

According to a recent survey, 58% of all CIO respondents believe that human error is their organization's most significant cybersecurity vulnerability [1]. Even though cybersecurity is widely recognized as a prevalent issue, surprisingly, many employees act irresponsibly in the workplace [2]. Different reasons for irresponsible security behavior have been discussed in the literature, including a lack of knowledge and skills, workplace stress [3], or the calculated risk of non-compliant behavior as the associated threat is considered unlikely to occur [4]. The latter reason plays an important role because it reduces the effectiveness of workplace interventions. For example, if employees have the knowledge and skills to comply with an organizational information security policy but are willing to take the risk and violate it for convenience reasons, security training can become ineffective. Literature has associated risk-taking with several terms: risk attitude, risk appetite, risk capacity, risk tolerance, risk aversion, and risk propensity [5, 6]. A common definition of risk-taking is the willingness of an individual to engage in or avoid risky behavior [6, 7]. A well-known measurement of risk-taking is the "DOSPERT" scale, which combines various contexts and distinguishes different practices (ethical, financial, health, safety, and social) through

17th International Conference on Wirtschaftsinformatik,
February 2022, Nürnberg, Germany

40 measures [8]. Beyond this, other measurements have been developed and tested in various contexts. For example, [9] provide an overview of measures used in the health setting. [10] developed a risk propensity scale measuring general risk-taking tendencies, and [11] developed a measurement in the context of finance.

Generally, risk propensity has been investigated for decision-makers of an organization [12], for an entire organization [13, 14], as well as for individuals in different contexts [15, 16]. For example, [17] investigated the relationship between general risk propensity and information security reinforcement intentions. [18] studied the influence that risk propensity has on CIO's decision-making process and [19] found that risk propensity significantly influences consumer's perceived privacy risk. [20] explored the relationship between perceived privacy risks and technology threats in the context of vehicles. The literature review indicates that the conceptualization of risk propensity differs in the literature. In this context, [21] distinguish risk-taking as a dispositional trait that is characterized as a stable individual attribute (e.g., risk averters or risk seekers) and risk-taking as a concept that is dependent on the specific situation to which the individual is exposed.

One theory that considers the willingness to take risks in the context of cybersecurity behavior is the technology threat avoidance theory (TTAT) [22]. The TTAT aims to explain how a perceived technology threat influences avoidance motivation and, ultimately, avoidance behavior. In a later study, [23] included risk tolerance in their model, which is defined as the minimal discrepancy that users are willing to accept between an unwanted end state and their current state. This discrepancy is also defined as the endurance of an individual to accept a certain level of risk (risk propensity). However, the scholars did not include this construct in the empirical validation process of TTAT. [7] were then the first to empirically test the influence of general risk propensity on threat perception based on the TTAT. General risk propensity was conceptualized in the study as a general extent to which individuals are willing to take risks in different life situations such as recreational activities, safety risks, financial risks, and social risks. The scholars found that general risk propensity significantly affects an individual's perceived threat severity, implying relevance in compliance behavior.

Against this background, our research follows the general idea that risk propensity influences an individual's technology threat avoidance behavior. Beyond that, and in alignment with [21], we also argue that risk propensity can be conceptualized as either a disposition or a situational concept, and both have different implications for individual technology threat avoidance behavior. To the best of our knowledge, literature has not investigated how situational risk propensity can influence an individual's technology threat avoidance behavior to the best of our knowledge. We argue that situational risk propensity is important to consider when studying technology threat avoidance behavior. The employee's workplace represents the situational context in this study. Security behavior in general can, for example, be influenced by the organizational risk appetite [24] or applied organizational punishments or rewards [3]. For this reason, we argue that situational risk propensity can differ from dispositional risk propensity. Therefore, we are inspired by the following research question: How

does situational risk propensity differ from dispositional risk propensity explaining individuals' technology threat motivations and behaviors?

We want to investigate the stated question by implementing an empirical research design based on the TTAT. Therefore, a data sample will be collected from employees and then be used to analyze our research model applying Partial Least Squares (PLS) structural equation modeling.

This research in progress proposal will briefly outline our research and is structured as follows: First, the theoretical foundations of the paper are described, the research model is set up, and the eleven hypotheses are developed. Finally, the main conclusions are presented.

2 Underlying Research Model based on the TTAT

TTAT is based on different theoretical considerations from the fields of psychology, healthcare, and information systems [22]. One popular theory it draws on is the protection motivation theory, which explains how individuals develop actions to defend themselves against threats. The TTAT shifts the focus to IT-related disciplines [25]. It proposes that IT users are willing to prevent a threat actively or passively by taking countermeasures if they think that the threat is avoidable and available countermeasures are effective [22].

[23] tested the theory in the context of spyware and anti-spyware software as the malicious IT and safeguarding measure, respectively. In this model, the avoidance behavior is influenced by a user's motivation to avoid malicious technology. Motivation, in turn, is affected by four antecedents: self-efficacy in one's own abilities, perceived effectiveness of safeguard measures, the costs of possible countermeasures against the threat, and the perceived scope and severity of the threat itself. The latter is affected by both an individual's subjective assessment of the threat's severity and their perceived vulnerability to the threat.

The following hypotheses describe the relationship of the basic model [7, 23]:

- H1a: Perceived susceptibility positively influences threat perceptions.
- H1b: Perceived severity partially mediates the influence that perceived susceptibility has on threat perceptions.
- H1c: Perceived severity positively influences threat perceptions.
- H2: Perceived threat positively influences avoidance motivation.
- H3: Safeguard effectiveness perceptions positively influence avoidance motivation.
- H4: Safeguard cost perceptions negatively influence avoidance motivation.
- H5: Self-efficacy about one's ability to implement a safeguard positively influences avoidance motivation.
- H6: Avoidance motivation positively influences avoidance behavior.

Various studies have been using the TTAT and its research model to explore different IT-related contexts, including security [7, 25–29].

In alignment with [7], we suggest including the concept of risk propensity as an antecedent of perceived threat. [7] have measured risk propensity as a disposition, i.e.,

the individual's general tendency to avoid or engage in risky behavior, which is reflected as the willingness to take risks in a variety of general life situations. The scholars argue that dispositional risk propensity is negatively related to threat perceptions because individuals with higher risk tendencies are less concerned about technology threats. We expect a similar effect of situational risk propensity on perceived threat. We argue that individuals adapt their risk behavior to the workplace situation, i.e., when the amount of risk that an organization tolerates in relation to cybersecurity is low (e.g., reflected by strict information security policies that are enforced with high penalties or rewards), individuals are more concerned about technology-related threats. We, therefore, suggest that situational risk propensity is negatively related to perceived threat. However, at the same time, we are also interested in how situational risk property mediates the relationship between risk propensity and perceived threat. We assume that situational risk propensity can weaken the relationship between dispositional risk propensity and threat perception because the situational context may influence dispositional risk propensity, i.e., the degree to which organizations tolerate risky behavior. Hence, dispositional risk propensity may become less relevant. We, therefore, propose the following hypotheses:

- H7: Dispositional risk propensity negatively influences threat perceptions.
- H8: Situational risk propensity positively or negatively influences threat perceptions.
- H9: Situational risk propensity mediates the relationship between dispositional relationship and threat perceptions.

Figure 1 presents our proposed research model.

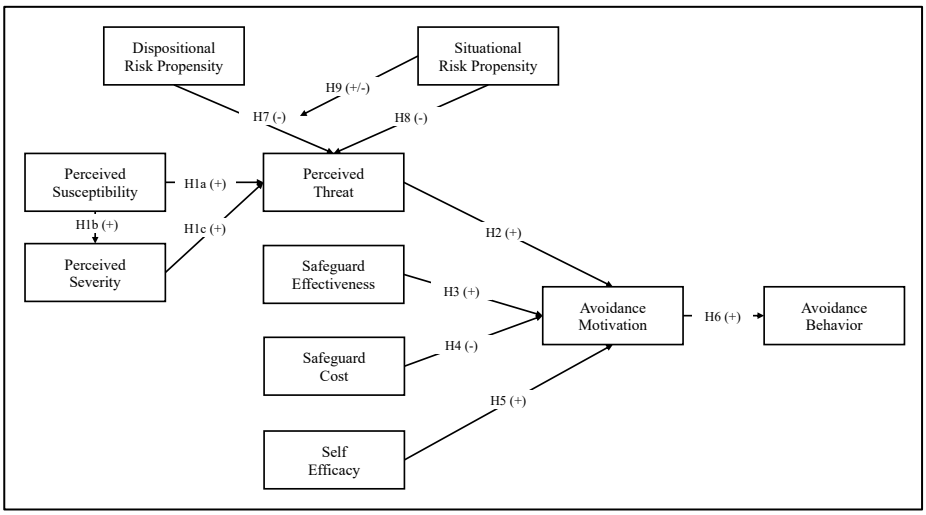

Figure 1: Research Model

Next, we plan to design an online survey based on our proposed research model. Here we will adopt the previously validated measures of [23] to assess all the original TTAT constructs and slightly modify them to our context. In line with our research

question, we will combine these measures with the ones of dispositional risk propensity proposed by [7] and additional items targeting situational risk propensity. The latter will include the quantity of information security guidelines and associated penalties or rewards as well as control measures and responsibilities. A final list of items is under development and will be published in the complete research paper.

All items of the questionnaire use a seven-point Likert scale (anchors: 1 = strongly disagree, 2 = disagree, 3 = somewhat disagree, 4 = neutral, 5 = somewhat agree, 6 = agree, and 7 = strongly agree).

We plan to use variance-based PLS structural equation modeling to evaluate the research model. We suggest adopting a two-step modeling approach by first assessing the quality of the measures and then testing the structural model [32].

Conclusion

This research in progress aims to understand how situational risk propensity influences the perceived threat and, consequently, the motivation and behavior toward avoiding technology threats based on the TTAT. In alignment with previous studies (e.g., [11], [13], [21], and [30], we argue that there are two types of risk propensity: situational and dispositional risk propensity. We hypothesize that situational risk propensity can influence threat perceptions, but it also mediates the relationship between dispositional risk propensity and threat perceptions. Our study has the potential to increase the understanding of how individuals adapt their situational risk propensity to workplace risk expectations. Therefore, our study can contribute to a better understanding of how to effectively design and manage cybersecurity solutions since our study emphasizes that the organization's risk propensity can influence an employee's risk propensity.

In the next step, we plan to collect data in German organizations. We propose using variance-based partial least structural equation modeling [31], utilizing SmartPLS to validate our measurements and the research model.

References

1. Mlitz, K. CISO: Biggest cyber vulnerability is human error 2021, https://www.statista.com/statistics/1259552/ciso-human-error-organization-cyber-vulnerability-by-country/ (Accessed: 10.12.2021)
2. Abu-Alhaija, M., Cyber Security: Between Challenges and Prospects (2020)
3. Trang, S., and Nastjuk, I.: Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. Computers & Security 104, pp. 1–15 (2021)
4. Vroom, C., von Solms, R.: Towards information security behavioural compliance. Computers & Security 23, pp. 191–198 (2004)
5. Berlinger, E., Váradi, K.: Risk Appetite. Public Finance Quarterly 60, pp. 49–62 (2015)
6. Hillson, D., Murray-Webster, R.: Using risk appetite and risk attitude to support appropriate risk-taking: a new taxonomy and model. Journal of Project, Program & Portfolio Management 2, pp. 29–46 (2011)

7. Carpenter, D., Young, D.K., Barrett, P., McLeod, A.J.: Refining Technology Threat Avoidance Theory. CAIS, pp. 380–407 (2019)
8. Blais, A.-R., Weber, E.U.: A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. Judgment and Decision Making 1 (2006)
9. Harrison, J.D., Young, J.M., Butow, P., Salkeld, G., Solomon, M.J.: Is it worth the risk? A systematic review of instruments that measure risk propensity for use in the health setting. Social Science & Medicine 60, pp. 1385–1396 (2005)
10. Meertens, R.M., Lion, R.: Measuring an Individual's Tendency to Take Risks: The Risk Propensity Scale. Journal of Applied Social Psychology 38, pp. 1506–1520 (2008)
11. Nicholson, N., Soane, E., Fenton-O'Creevy, M., Willman, P.: Personality and domain-specific risk taking. Journal of Risk Research 8, pp. 157–176 (2005)
12. Sitkin, S.B., Weingart, L.R.: Determinants of Risky Decision-Making Behavior: A Test of the Mediating Role of Risk Perceptions and Propensity. AMJ 38, pp. 1573–1592 (1995)
13. Harwood, I.A., Ward, S.C., Chapman, C.B.: A grounded exploration of organisational risk propensity. Journal of Risk Research 12, pp. 563–579 (2009)
14. Walls, M.R., Dyer, J.S.: Risk Propensity and Firm Performance: A Study of the Petroleum Exploration Industry. Management Science 42, pp. 1004–1021 (1996)
15. Hatfield, J., Fernandes, R.: The role of risk-propensity in the risky driving of younger drivers. Accident Analysis & Prevention 41, pp. 25–35 (2009).
16. Warkentin, M., Goel, S., Williams, K. J., & Renaud, K.: Are we predisposed to behave securely? Influence of risk disposition on individual security behaviours. In 26th European Conference on Information Systems (2018)
17. Nguyen, Q.N., Kim, D.J.: Enforcing Information Security Protection: Risk Propensity and Self-Efficacy Perspectives. In Hawaii International Conference on System Sciences (2017)
18. Villarreal, M.A., Ozuna, T., Tanguma, J.: CIO executive risk behavior model. In Americas Conference on Information Systems (2009)
19. Xu, B., Lin, Z., Shao, B.: Factors affecting consumer behaviors in online buy-it-now auctions. Internet Research 20, pp. 509–526 (2010)
20. Koester, N., Cichy, P., Antons, D., Salge, T.: Privacy Risk Perceptions in the Connected Car Context. Hawaii International Conference on System Sciences (2021)
21. Das, T.K., Teng, B.-S.: Strategic risk behaviour and its temporalities: between risk propensity and decision context. Journal of Management Studies 38, pp. 515–534 (2001)
22. Liang, H., Xue, Y.: Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly 33, pp. 71–90 (2009)
23. Liang, H., Xue, Y.: Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the association for information systems 11(7), pp. 394-413 (2010)
24. Feng, C. Q., & Wang, T.: Does CIO risk appetite matter? Evidence from information security breach incidents. International Journal of Accounting Information Systems 32, pp. 59–75 (2019)
25. Boysen, S., Hewitt, B., Gibbs, D., McLeod, A.: Refining the Threat Calculus of Technology Threat Avoidance Theory. CAIS, pp. 95–104 (2019)
26. Arachchilage, N.A.G., Love, S.: A game design framework for avoiding phishing attacks. Computers in Human Behavior 29, pp. 706–714 (2013).
27. Chen, Y., Zahedi, F.M.: Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. MISQ 40, pp. 205–222 (2016)

28. Mwagwabi, F., McGill, T., Dixon, M.: Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines, in 47th Hawaii International Conference on System Sciences (2014)
29. Young, D., Carpenter, D., McLeod, A.: Malware Avoidance Motivations and Behaviors: A Technology Threat Avoidance Replication. AIS TRR 2 pp. 1–17 (2016)
30. Huff, R.A., Keil, M., Kappelman, L., Prybutok, V.: Validation of the Sitkin-Weingart Business Risk Propensity Scale. Management Research News 20, pp. 39–48 (1997)
31. Lohmöller, J.-B.: Latent Variable Path Modeling with Partial Least Squares. Springer Science & Business Media (2013)
32. Anderson, J.C. and Gerbing, D.W.: Structural equation modeling in practice: A review and recommended two-step approach. Psychological bulletin, 103(3), p. 411 (1988)