The Eurasia Proceedings of
Educational and Social Sciences (EPESS)
ISSN: 2587-1730

The Eurasia Proceedings of Educational and Social Sciences (EPESS), 2026

Volume 48, Pages 1-7

IConMEB 2026: International Conference on Management Economics and Business

Domain-Specific Risk Perception in IT Security Decisions: Empirical Examination of the Modified Domain-Specific Risk-Taking (DOSPERT) Framework

Pal Feher-Polgar
Obuda University

Peter Szikora
Obuda University

Abstract: The aim of this paper is to examine the applicability of a modified version of the Domain-Specific Risk-Taking (DOSPERT) questionnaire for measuring risk-taking decisions related to IT security. Based on a domain-specific decision theory approach, the research analyzes the internal structure of decisions related to information and communication technologies (ICT), with a particular focus on the role of perceived benefits, perceived risks, and the probability of action. The empirical study was conducted with 772 university students using a self-reported questionnaire. The results show that IT security risk-taking is primarily explained by perceived benefits, while the role of perceived risk and probability of action becomes secondary in a multivariate model. Based on psychometric analyses, the inclusion of the ICT-specific domain is theoretically justified in the DOSPERT framework, but further refinement of the measurement tool is warranted to more accurately capture the specificities of IT security decisions. The study contributes to the intersection of behavioral decision theory and information systems research by focusing on theoretical and methodological issues in the measurement of risk decisions.

Keywords: Domain-specific risk-taking, IT security decisions, DOSPERT questionnaire, Risk perception

Introduction

The everyday use of information and communication technologies (ICT) has fundamentally transformed the environment for individual and organizational decision-making in recent decades. The widespread use of digital devices, online platforms, and network services has created decision-making situations in which risks are often not immediately apparent, their effects are delayed, and their consequences cannot be linked to a single specific decision. A significant portion of the risks associated with IT security therefore do not stem solely from technical vulnerabilities, but are closely related to user behavior, routines, and decisions (Keszthelyi, 2022; Szikora & Ali, 2017). In this sense, IT security can be interpreted not only as a technological issue, but also as a question of decision theory and behavioral science.

The study of risk-taking behavior is a central area of research in decision theory and behavioral science. Early approaches typically treated risk-taking as a general personality trait, but empirical findings consistently suggest that individuals' risk decisions are highly dependent on the specific decision situation and domain under consideration. This realization led to the development of the theoretical framework of domain-specific risk-taking, according to which risk-taking propensity is not a uniform personality trait but manifests itself in different forms in different risk domains (Blais & Weber, 2006).

One of the best-known empirical tools of the domain-specific approach is the Domain-Specific Risk-Taking (DOSPERT) scale, which measures risk-taking across several distinct domains and distinguishes three basic

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

decision dimensions: perceived benefit, probability of action, and perceived risk (Blais & Weber, 2006). One of the key contributions of DOSPERT is that it allows for the separate examination of these dimensions, thereby providing a more nuanced picture of the decision-making mechanisms underlying risk-taking behavior (Blankenstein et al., 2024). Numerous empirical studies have also shown that in certain domains, perceived benefits are a stronger explanatory factor for risk-taking than perceived risk itself, especially in decision-making situations where the negative consequences are abstract or delayed (Guenther et al., 2024).

Decisions related to IT security typically create such a decision-making environment. Users' everyday digital practices—such as using public networks, managing access data, or transferring data to personal devices—are often routine and low in awareness, while the potential consequences can be severe (Szikora & Ali, 2017; Keszthelyi, 2022). Information security research emphasizing the role of the human factor consistently points out that technical protection solutions alone are not sufficient, as user decisions and perceptions fundamentally influence the effectiveness of security systems (National Media and Infocommunications Authority, 2020; Lazányi & Hajdú, 2017).

Despite all this, risks related to IT security appear only to a limited extent explicitly in the traditional domain structure of the DOSPERT questionnaire. This raises the question of the extent to which the decision-making dimensions distinguished by DOSPERT are able to capture the specificities of IT security decisions, and whether the role of these dimensions differs from the patterns observed in general risk areas. A particularly relevant question is which psychological factors are decisive in IT security risk-taking: do perceived risks or rather short-term perceived benefits dominate decision-making?

The aim of this study is to empirically test a modified version of the DOSPERT questionnaire by adding a new domain related to IT security. The research analyzes the relationship between perceived benefits, perceived risks, and the probability of action in relation to IT security risk-taking among university students. The results of the study contribute to the theoretical refinement of domain-specific risk-taking and provide an empirical basis for understanding IT security decisions from a behavioral science perspective, with a particular focus on the role of benefit-driven decision-making logic.

Literature Review

The study of risk-taking decisions is a key area of research in decision theory and behavioral science, which has long been based on the assumption that individuals' attitudes toward risk are relatively stable and can be interpreted as personality traits. However, these approaches had limited explanatory power in decision-making situations where the nature, timing, and perceptibility of risks differed significantly. Empirical findings have led to an increasing emphasis on a domain-specific approach, according to which risk-taking is not a uniform behavioral pattern but varies depending on the decision-making context (Blais & Weber, 2006).

One of the most important contributions of the domain-specific approach is the recognition that risk-taking decisions do not arise solely from the perception of danger but are complexly linked to the benefits associated with the behavior in question and the subjective feasibility of the action. The Domain-Specific Risk-Taking (DOSPERT) questionnaire is an empirical operationalization of these theoretical insights, examining risk-taking along three distinct decision dimensions: perceived benefit, perceived risk, and action probability (Blais & Weber, 2006). One of the basic assumptions of the model is that the effects of these dimensions are not necessarily equal and that their roles may vary in importance depending on the domain.

Numerous empirical studies have shown that in certain risk areas, perceived benefit is a stronger predictor of risk-taking behavior than perceived risk itself. This is particularly true in decision-making situations where negative consequences are delayed or difficult to link to a single specific decision. In such cases, individuals tend to overestimate the immediately perceptible benefits, while the behavior-shaping power of potential losses is reduced (Blankenstein et al., 2024; Guenther et al., 2024). This benefit-oriented decision-making logic has appeared in several domains, especially in the case of abstract or technologically mediated risks.

Decisions related to information and communication technologies have a number of characteristics that favor the development of benefit-driven decision-making patterns; In this regard, the literature also points out that behavioral patterns in the digital space—such as internet use and its psychological consequences—have a complex influence on decisions, including the psychological links between internet addiction and loneliness (Nincevic, 2025; Cigdem, 2016). In contrast, the benefits associated with these behaviors—such as convenience, speed, or functionality—are immediate and tangible (Keszthelyi, 2022; Szikora & Ali, 2017). This asymmetry

raises the possibility that, in the case of IT security decisions, classic risk perception mechanisms have limited explanatory power.

The information security literature is placing increasing emphasis on the human factor, recognizing that the effectiveness of technical protection solutions depends largely on user decisions and behaviors (National Media and Communications Authority, 2020; Lazányi & Hajdú, 2017). However, these approaches often interpret risks at the ad hoc or organizational level and focus less on the structural patterns of individual decision-making dimensions in the specific context of IT security. As a result, it remains an open question to what extent the decision-making dimensions identified by DOSPERT are able to capture the specificities of IT security risk-taking.

This study joins the discourse in the literature at this point and undertakes to empirically examine the decision-making structure of IT security risk-taking using the DOSPERT framework. The focus is not on exploring demographic differences, but on the relative roles of perceived benefits, perceived risks, and probability of action in explaining ICT security risk-taking. Based on the literature, it can be assumed that decisions in this domain are primarily organized according to benefit-oriented logic, while the role of risk perception and probability of action is more complex and requires empirical investigation.

Research Questions and Hypothesises

Risk-taking related to IT security occurs in a decision-making environment that differs in several respects from situations examined in the classic risk domain. Decisions related to the use of digital tools are often routine, the potential negative consequences are delayed, and in many cases cannot be linked to a single specific action. Based on these characteristics, it can be assumed that the decision-making mechanisms behind IT security risk-taking operate with different weightings than in traditional risk areas.

The Domain-Specific Risk-Taking (DOSPERT) framework allows us to examine the decision-making dimensions that make up risk-taking—perceived benefit, perceived risk, and probability of action—separately. At the same time, it remains unclear in the field of IT security what relative role these dimensions play in the development of risk-taking behavior and whether their impact is equal in this specific decision-making context. The primary objective of this study is therefore to empirically examine the relationship between the decision-making dimensions identified by DOSPERT and risk-taking related to IT security. Accordingly, the following research question was formulated:

RQ: What relationship can be observed between perceived benefits, perceived risks, probability of action, and risk-taking related to IT security?

Based on empirical results published in the literature, it can be assumed that directly perceptible benefits play a more decisive role in IT security decisions than abstract or delayed risks. Accordingly, the following hypotheses were formulated:

H1 (Perceived Benefit Hypothesis): The perceived benefit has a positive and significant relationship with IT security risk-taking.

In the theoretical framework of the DOSPERT model, perceived risk appears as a deterrent, but in the field of IT security, risks are often less tangible, which can reduce their behavioral influence. Based on this, the following hypothesis was formulated:

H2 (Perceived Risk Hypothesis): The perceived risk is negatively correlated with IT security risk-taking.

The probability of action dimension expresses the extent to which individuals consider the implementation of a given behavior to be realistic, which can be an independent component of the decision-making process, especially in the case of routine behaviors. The following hypothesis was developed for its empirical examination:

H3 (Likelihood of Action Hypothesis): The probability of action is positively correlated with IT security risk-taking.

The above research question and hypotheses make it possible to examine the decision-making structure underlying IT security risk-taking and to determine which of the dimensions identified by DOSPERT are decisive in this specific domain.

Methodology

The aim of the research was to empirically examine risk-taking related to IT security using the Domain-Specific Risk-Taking (DOSPERT) framework. Data collection was quantitative, cross-sectional, and based on a self-reported questionnaire. The study was conducted in November 2025 among students at a Hungarian higher education institution. Sampling was convenience-based, and data collection took place in the context of courses related to educational activities. Participation was voluntary and anonymous; respondents were informed in advance about the purpose of the research and that the data would be used exclusively for research purposes. The final analysis included a sample of 772 individuals. The age of the respondents ranged from 17 to 46 years, with a mean age of 21.44 years (SD = 2.65). The gender distribution of the sample was asymmetrical, with 82.8% of participants being male (n = 639) and 17.2% female (n = 133). The composition of the sample showed an age concentration typical of the higher education student population, which is consistent with the exploratory and validation objectives of the study.

The measurement tool used in the research was a modified version of the Domain-Specific Risk-Taking (DOSPERT) questionnaire. The original DOSPERT questionnaire measures risk-taking across multiple risk domains and distinguishes three basic decision dimensions: perceived benefit, perceived risk, and probability of action. The present study was based on the DOSPERT version adapted into Hungarian by István Radnóti. The questionnaire was modified so that risk-taking related to IT security could also be examined in a separate, domain-specific form. The modified questionnaire included a new IT security domain, which initially consisted of five situational items related to everyday digital device use. These items represented typical IT security risks, such as forwarding company data to a private email address, using public Wi-Fi networks, or copying work data to a mobile phone. The wording of the items was consistent with the original DOSPERT questions in terms of content and structure so that respondents could interpret them within a uniform decision-making framework. A 7-point Likert scale was used for each item in the questionnaire. For the perceived benefit dimension, the scale ranged from "no benefit" to "significant benefit." For the action probability dimension, respondents could give their answers between the endpoints "never, under any circumstances" and "definitely." The perceived risk dimension was measured between the endpoints "no risk" and "highly risky."

During the empirical examination of the items in the IT security domain, one item was removed from the final scale due to low correlation, so a composite indicator consisting of four items (IKT4_Atlag) was ultimately developed to measure IT security risk-taking. The internal reliability of the scale was examined using Cronbach's alpha, which showed a moderate value ($\alpha = 0.52$), but the use of alternative reliability measures was beyond the exploratory objectives of this study. Considering the low number of items in the scale, the situational nature of the items, and the heterogeneity of behaviors, this value can be considered acceptable in an exploratory, domain-specific study. To explore the scale structure, we used exploratory factor analysis with principal axis factorization and oblique rotation, which confirmed a single-factor structure for the finalized item set.

The first step in the data analysis was data verification and descriptive statistical analysis. Pearson's correlation analysis was used to examine the relationships between the main variables. To test the research questions and hypotheses, we performed multivariate linear regression analysis, in which risk-taking related to IT security (IKT4_Atlag) was used as the dependent variable, while perceived benefits, perceived risks, and probability of action were used as explanatory variables. The analyses were performed using IBM SPSS Statistics 25 software.

Results

As a first step in the analysis, descriptive statistics and Pearson correlation analyses were performed to explore the relationship between IT security risk-taking and the decision-making dimensions of the Domain-Specific Risk-Taking (DOSPERT) questionnaire. The average composite indicator measuring IT security risk-taking (IKT4_Atlag) was 3.36 (SD = 1.05), which falls in the middle range of the 7-point scale and indicates a moderate willingness to take risks.

The results of the correlation analyses are summarized in Table 1. IT security risk-taking showed a strong positive correlation with the perceived benefit dimension ($r = 0.676$; $p < 0.001$) and a moderate positive correlation with the probability of action ($r = 0.513$; $p < 0.001$). In contrast, perceived risk showed a weak but statistically significant negative correlation with IT security risk-taking ($r = –0.251$; $p < 0.001$). These results suggest that, at the bivariate level, all three decision dimensions are significantly related to IT security risk-taking, but the direction and strength of the correlations differ.

Table 1. Descriptive statistics and Pearson correlations between ICT risk-taking and DOSPERT dimensions (N = 772)

Dimenson	M	SD	1	2	3	4
1. ICT4_Avg	3,36	1,05	—			
2. Benefits_Avg	2,98	0,65	,676***	—		
3. Probability_Avg	3,07	0,67	,513***	,760***	—	
4. Risk_Avg	4,64	0,67	−,251***	−,423***	−,384***	—

Note: *** p < 0,001

To examine the relative explanatory power of the decision dimensions, we used multivariate linear regression analysis, in which IT security risk-taking (IKT4_Atlag) was the dependent variable, while perceived benefit, perceived risk, and probability of action were the explanatory variables. The regression model was statistically significant ($F(3, 768) = 228.41$; $p < 0.001$) and explained 47.2% of the variance in the dependent variable ($R^2 = 0.472$), indicating a strong model fit.

Based on the regression coefficients, the perceived benefit proved to be an exceptionally strong and significant predictor ($\beta = 0.697$; $p < 0.001$), indicating that the increase in IT security risk-taking can be explained primarily by the strengthening of the benefits associated with the given behaviors. In contrast, neither perceived risk ($\beta = 0.041$; $p = 0.19$) nor probability of action ($\beta = 0.021$; $p = 0.66$) showed a statistically significant effect in the model when controlling for the effects of other decision dimensions. Mathematically, this means that the t-tests for the regression coefficients did not reach the significance level ($|t| < 1.96$), so the null hypothesis could not be rejected in these cases.

The summary results of the empirical testing of the hypotheses are presented in Table 2. Hypothesis H1, which assumed a positive relationship between perceived benefits and IT security risk-taking, received clear empirical support. Hypothesis H2, which assumed a negative effect of perceived risk, was supported at the bivariate level, but did not prove significant in the multivariate regression model and was therefore rejected. Similarly, hypothesis H3 was not empirically confirmed, as the explanatory power of the probability of action disappeared in the model.

Table 2. The summary results of the empirical testing of the hypotheses

Hypothesis	Predictor	Expected direction	Empirical result	Status
H1	Perceived benefit	positive	$\beta = 0,697$, $p < 0,001$	Accepted
H2	Perceived risk	negative	n.s.	Rejected
H3	Probability of action	positive	n.s.	Rejected

From a mathematical point of view, these results suggest that a single predictor, perceived benefit, explains the majority of the variance in IT security risk-taking, while the effect of other decision dimensions is largely mediated through the interaction between predictors. The discrepancy between the correlation and regression results suggests that the effects of perceived risk and probability of action are not independent, but manifest themselves indirectly in IT security decisions, primarily through their relationship with perceived benefits.

Discussion

The aim of this study was to explore the decision-making dimensions of IT security risk-taking and to assess the suitability of the Domain-Specific Risk-Taking (DOSPERT) framework for empirical research in this specific domain. The results clearly show that the decision-making structure of IT security risk-taking is not balanced across the dimensions identified by DOSPERT but is organized along a distinctly profit-oriented logic. Based on multivariate regression analyses, perceived benefit was the only decision dimension that had independent and strong explanatory power with regard to IT security risk-taking. This result is consistent with previous empirical findings that in abstract, technologically mediated risk environments, individuals' decisions are primarily structured by directly perceptible benefits, while the behavior-shaping power of potential losses is reduced. In

the case of IT security decisions, convenience, speed, and functionality represent immediate benefits that can become dominant even if users are theoretically aware of the associated risks. It is particularly noteworthy that although perceived risk and probability of action were significantly related to IT security risk-taking at the bivariate level, these effects disappeared in the multivariate model. This result suggests that the effect of these dimensions is not independent, but primarily through their association with perceived benefits. In other words, in the case of IT security decisions, risk perception alone is not sufficient to reduce risk-taking if the benefits associated with the behavior remain dominant.

This observation has important theoretical implications for the applicability of the DOSPERT framework. Although the model theoretically treats perceived benefits, perceived risk, and action probability as equal decision dimensions, the present results suggest that the empirical weight of these dimensions may vary significantly across domains. In the field of IT security, the decision structure is asymmetrical, with the benefit dimension playing a dominant role, while risk perception and action probability appear as secondary, indirect factors. This supports the view that domain-specific interpretation and separate treatment of the relative weights of the dimensions may be justified when applying DOSPERT.

The results of the study are also relevant from a practical point of view. IT security awareness programs and training courses are often based on emphasizing risks, if awareness of the dangers alone has a deterrent effect. In contrast, the present results suggest that such approaches may have limited effectiveness if they do not address the reduction of benefits associated with risky behaviors or offer alternative benefits. When designing IT security interventions, it may therefore be advisable to focus on restructuring decision benefits, for example by emphasizing the tangible benefits of safe behavior. Among the limitations of the study are the cross-sectional research design and the student sample, which limit the generalizability of the results. In addition, the internal reliability of the scale used to measure the IT security domain was moderate, which can be explained by the heterogeneity and situational nature of the behaviors examined. However, these limitations do not detract from the validity of the results, but rather point to further research directions, particularly with regard to refining the measurement tool and applying longitudinal studies.

Overall, this study contributes to the behavioral science understanding of IT security risk-taking by empirically confirming the dominance of utility-driven decision-making logic in this domain. The results confirm that IT security decisions are not based solely on risk recognition, but are organized along complex, asymmetric decision structures in which immediate benefits play a decisive role.

Conclusions and Implications

The aim of the study was to empirically examine the decision-making dimensions underlying IT security risk-taking and to assess the suitability of the Domain-Specific Risk-Taking (DOSPERT) framework for describing this specific domain. The results clearly show that IT security risk-taking is not structured in a balanced way based on the dimensions of perceived benefit, perceived risk, and probability of action, but is structured along a distinctly benefit-driven decision-making logic.

Based on multivariate analyses, perceived benefits proved to be the only independent and strong explanatory factor for IT security risk-taking, while the role of perceived risk and probability of action proved to be secondary and indirect. From a theoretical point of view, this result contributes to the literature on domain-specific risk-taking by empirically supporting the hierarchical weighting of decision dimensions, which varies from domain to domain. The DOSPERT framework thus provides a suitable starting point for examining IT security decisions, but the results suggest that interpreting the relative roles of the dimensions is essential in this context. As a practical implication, the results of the study draw attention to the fact that IT security awareness programs alone may be of limited effectiveness if they focus solely on emphasizing risks. A more effective approach may be interventions that focus on reducing the benefits associated with risky behaviors and demonstrating the tangible benefits of safe alternatives. Limitations of the study include its cross-sectional design and student sample, which limit the generalizability of the findings, but also provide a clear direction for future research toward refining the measurement tool and conducting longitudinal studies.

Scientific Ethics Declaration

Conflict of Interest

* The authors declare that they have no conflicts of interest.

Funding

* This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements or Notes

* This article was presented as an oral presentation at the International Conference on Management Economics and Business (www.iconmeb.net) held in Budapest/Hungary on February 05-08, 2026

References

Blais, A. R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making, 1*(1), 33–47.

Blankenstein, N. E., van Hoorn, J., Dekkers, T. J., Popma, A., Jansen, B. R., Weber, E. U., & van Duijvenvoorde, A. C. K. (2024). Adolescent risk-taking likelihood, risk perceptions, and benefit perceptions across domains. *Personality and Individual Differences, 231*, 112806.

Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological Bulletin, 125*(3), 367–383.

Cigdem, H., Yildirim, O. G., & Erdogan, T. (2016). The analysis of relationship between students' internet addiction and miscellaneous variables. *The Eurasia Proceedings of Educational and Social Sciences, 5,* 203-205.

Guenther, B., Galizzi, M. M., & Sanders, J. G. (2024). PDOSPERT: A new scale to predict domain-specific risk-taking behaviors in times of a pandemic. *Journal of Behavioral Decision Making, 37*, e2413.

Keszthelyi, A. (2022). Some special results of ICT revolution. In Živan, Ž. (Ed.), *XVIII International May Conference on Strategic Management – IMCSM22* (pp. 479–484). University of Belgrade, Technical Faculty in Bor, Management Department.

Lazányi, K., & Hajdu, B. (2017). Trust in human–robot interactions. In *2017 IEEE 14th International Scientific Conference on Informatics* (pp. 216–220). IEEE.

Nemzeti Média- és Hírközlési Hatóság. (2020). *Magyarország kiberbiztonsági helyzete*. NMHH.

Nincevic, M. M. (2025). Digital loneliness and internet addiction: Educational challenges for mental health. *The Eurasia Proceedings of Educational and Social Sciences, 47,* 201-214.

Sowan, W. (2023). Gender differences in expectations in risk situations. *Deviant Behavior*, *44*(11), 1598-1606.

Szikora, P., & Ali, M. (2017). Az Y generáció és az internet kapcsolata. In *Tanulmánykötet – Vállalkozásfejlesztés a XXI. században VII.* (pp. 11–23)

Author(s) Information

Pal Feher-Polgar
Obuda University Keleti Károly Faculty of Business and Management, 1084, Tavaszmező str. 17, Budapest, Hungary.
ORCID iD: https://orcid.org/0000-0002-4650-5253
*Contact e-mail: *feherpolgar.pal@kgk.uni-obuda.hu*

Peter Szikora
Obuda University Keleti Károly Faculty of Business and Management, 1084 Tavaszmező str. 17, Budapest, Hungary.
ORCID iD: https://orcid.org/0000-0001-8680-3880

*Corresponding authors contact email

To cite this article:

Feher-Polgar, P., & Szikora, P. (2026). Domain-specific risk perception in IT security decisions: Empirical examination of the modified DOSPERT framework. *The Eurasia Proceedings of Educational and Social Sciences (EPESS), 48,* 1-7.