Issues in Information Systems
Volume 25, Issue 3, pp. 1-12, 2024

DOI: https://doi.org/10.48009/3_iis_2024_101

Risk-taking propensity and information security compliance behavior in government workers

Tammy Ferrante, *University of Charleston, TammyFerrante@ucwv.edu*
Taiwo Ajani, *University of Charleston, TaiwoAjani@ucwv.edu*

Abstract

This study explores the intersection of risk-taking behavior and information security compliance within the context of a federal agency, aiming to illuminate the impact of individual behaviors on cybersecurity efforts. Amidst rising expenditures on information security by both corporations and governments, and an increasing trend of sophisticated cyber-attacks, this research underscores the critical role of the human factor in safeguarding digital assets. Utilizing a quantitative correlational methodology grounded in the Knowledge, Attitudes, and Behaviors (KAB) and Risk Propensity Model (RPM) frameworks, this study engaged 127 federal employees to examine the correlation between their propensity to take risks and their adherence to information security policies. Through descriptive statistics and multiple regression analysis, the study found that risk-taking propensity significantly influences information security compliance, contrary to age, which showed no significant effect. These findings suggest that enhancing organizational cybersecurity can be achieved by focusing on the individual risk profiles of employees, proposing the development of targeted strategies to address and mitigate risk-taking behaviors. This research contributes to the ongoing discourse on optimizing information systems for improved organizational performance and highlights the necessity of integrating psychological dimensions into cybersecurity management strategies.

Keywords: User Behavior, KAB Model, RPM Framework, Insider Threats, Compliance Behavior, Human Aspects of Information Security, Risk Management, Cybersecurity, Multiple Regression

Introduction

In an era where cybersecurity threats are increasingly sophisticated and widespread, organizations worldwide, including governmental bodies, are channeling significant resources towards bolstering their information security measures, focusing on confidentiality, integrity, and availability (CIA). This strategic emphasis often necessitates dependence on sophisticated software solutions, stringent access controls, and comprehensive information security policies to mitigate potential breaches (Nasir et al., 2019). Despite these efforts, the intricacy of software management and the reliance on standardized security measures may not fully shield organizations from the multifaceted threats posed by cyber attackers. This challenge underscores the pivotal role of human behavior in the cybersecurity ecosystem, where individuals' actions or inactions can significantly impact an organization's security posture (McCormac et al., 2017).

As the scale of cyber threats escalates, with projections suggesting a potential loss exceeding $6 trillion globally by 2021 due to data breaches, there is a heightened urgency to delve into the human factors that influence cybersecurity (Khando et al., 2021). Notably, the most severe breaches often stem from within, driven by employees' actions, whether inadvertent or deliberate, underscoring the necessity of fostering a robust culture of security compliance (Safa et al., 2018). This growing concern necessitates a deeper understanding of not just general human behaviors, but also specific traits such as risk-taking propensities and demographic factors like age, and how they correlate with information security compliance behaviors within a federal agency setting.

In light of these considerations, this study adopts a quantitative correlational approach to examine the relationships between employees' risk-taking behaviors and their compliance with information security protocols, as well as the influence of age on these compliance behaviors, within a federal agency setting (Dalal et al., 2021). Drawing upon the Knowledge, Attitudes, and Behaviors (KAB) model and the Risk Propensity Model (RPM), this research aims to provide empirical insights into how individual behaviors, demographic factors, and attitudes towards cybersecurity can be leveraged to enhance organizational security measures. By focusing on a cohort of federal employees, this investigation sought to contribute to the broader discourse on optimizing information system security in governmental agencies, thereby aligning with the overarching mission of strengthening both organizational performance and security through informed human-centered strategies.

This research underscores the imperative of integrating behavioral insights into the cybersecurity management framework, advocating for an approach that considers employees not merely as potential security risks but as integral partners in the collective endeavor to fortify cyber defenses (Hadlington, 2018). Through this lens, the study endeavors to elucidate the critical intersections between human behavior, demographic characteristics, and technological safeguards, aiming to inform the development of more effective, adaptive, and human-centric cybersecurity strategies for governmental and organizational resilience.

Statement of the Problem

This study addresses the critical gap in understanding the impact of employees' risk-taking behaviors on information security compliance within federal agencies. Despite significant investments in cybersecurity measures, the human element remains a potential vulnerability, with existing strategies primarily focused on technical solutions rather than a holistic approach that integrates human behavior. This research aims to explore the extent to which risk-taking propensity among federal employees influences their adherence to information security protocols, thereby highlighting the need for a comprehensive cybersecurity strategy that encompasses technology, organizational factors, and, crucially, human behavior. By examining this relationship, the study seeks to inform the development of more effective, multifaceted cybersecurity frameworks that enhance protection against both internal and external threats, aligning with the mission to improve organizational performance and security through informed, human-centered strategies.

Purpose of the Study

This study is designed to explore the dynamic interplay between federal employees' risk-taking behaviors and their adherence to information security policies, with a goal of informing a more integrated and effective cybersecurity strategy. Amid rising incidents and costs associated with data breaches, largely attributed to user behavior, there's a pressing need for a deeper understanding of how human factors influence cybersecurity outcomes. By employing a quantitative correlational approach, utilizing online questionnaires through Qualtrics, and analyzing responses with multiple regression analysis, this research aims to quantify the relationship between employees' propensity to take risks and their compliance with security protocols.

Leveraging validated instruments such as the Human Aspects of Information Security Questionnaire (HAIS-Q) and Risk-Taking Propensity Scale (RTPS), the study seeks to provide actionable insights that can enhance the design and implementation of cybersecurity measures, emphasizing the critical role of human behavior in strengthening security frameworks within federal agencies. This approach aligns with our mission to enhance organizational performance and security posture through the thoughtful integration of technology, organizational strategies, and a nuanced understanding of human factors.

Specifically, the research questions are:

> **RQ1:** *To what extent does risk-taking propensity covary with information security compliance behavior in a federal agency?*
> **RQ2:** *To what extent does age covary with information security compliance behavior in a federal agency?*

Introduction to Theoretical Framework

This study embarks on a quantitative correlational investigation to discern the correlation between federal employees' inclination towards risk-taking and their commitment to adhering to information security protocols. Central to this exploration is the integration of the Knowledge, Attitudes, and Behaviors (KAB) model with the Risk Propensity Model (RPM), offering a multifaceted lens through which the dynamics of cybersecurity compliance behaviors are examined (McCormac et al., 2017). The KAB model posits that an enhancement in a user's cybersecurity awareness is intrinsically linked to an elevation in their security-minded actions, suggesting a direct pathway from knowledge acquisition to behavioral modification in the context of information security. Complementing this, the RPM delves into the innate tendencies of individuals towards risk, exploring how these predispositions influence one's adherence to cybersecurity measures.

The convergence of the KAB and RPM models in this study is deliberate, aiming to illuminate the complex interplay between an individual's cybersecurity knowledge, their attitudes towards risk, and the manifestation of these elements in their security compliance behaviors. This analytical framework is poised to unravel the nuanced ways in which awareness and risk tolerance coalesce to shape cybersecurity practices within federal agencies. Such an endeavor aligns with our mission to enhance the efficacy of information systems in supporting organizational objectives and improving the educational process around cybersecurity, by highlighting the critical role of human factors in the broader cybersecurity landscape (Hadlington, 2018).

By marrying the insights derived from the KAB and RPM models, this research intends to provide a deeper understanding of the psychological underpinnings of cybersecurity compliance, thus paving the way for the development of more targeted, effective strategies to bolster security measures. This approach acknowledges the imperative of going beyond technological solutions to incorporate a comprehensive understanding of human behavior, thereby fostering a more resilient, informed approach to combating cyber threats within the governmental sector (Nasir et al., 2019).

This study also employs the KAB model to investigate the relationship between information security awareness and the level of safe conduct exhibited by individuals. The RPM, in turn, provides a lens to examine the role of risk-taking tendencies in influencing compliance with cybersecurity protocols (McCormac et al., 2017). By integrating these models, the research aims to offer a comprehensive view of how knowledge, attitudes, and behaviors intersect with risk propensities to impact information security compliance (Liu et al., 2018).

Methodology

Adopting a quantitative framework facilitated the examination of statistical relationships between the identified variables, utilizing numerical data to construct and test hypotheses. The closed-ended nature of quantitative research, through survey methods, allowed for the analysis of larger sample sizes, thereby enabling more statistically significant conclusions.

Research Design and Rationale

The study employed a non-experimental and correlational design, focusing on identifying potential statistical correlations without manipulating variables, which could introduce ethical concerns. This approach was optimal for investigating the relationships between key variables, including users' knowledge on Information Security Awareness (ISA), their perceptions of cybersecurity, and their adherence to or deviation from compliant behaviors.

Population and Sample

The targeted population included 642 employees and contractors of a federal agency in the United States with authorized network access. A convenience sampling strategy was used, and the sample size was determined through an a priori power analysis, resulting in a minimum requirement of 120 participants to achieve a statistical power of 0.80.

Instrumentation

Data were collected via an online survey distributed through Qualtrics, comprising 37 questions derived from the Human Aspects of Information Security Questionnaire (HAIS-Q) and the Risk-Taking Propensity Scale (RTPS). These instruments were chosen for their previous validation and relevance to the theoretical foundation of the study, the Knowledge, Attitudes, and Behaviors (KAB) model.

Operational Definitions and Variables

The study operationalized information security compliance behavior and risk-taking propensity through the RSCB and RTPS, respectively. Compliance behavior was gauged by the sum of scores on 20 Likert-type items, while risk-taking propensity was assessed through 14 Likert-type items from the RTPS.

Procedures and Ethical Considerations

Ethical adherence was paramount, with procedures designed to protect participant anonymity and data integrity. Informed consent was obtained electronically, with participants aware of their right to withdraw at any time. Data collection and storage were conducted following stringent security protocols to ensure confidentiality.

Data Analysis

The analysis involved a multifaceted approach, starting with profile characteristics and descriptive statistics, followed by tests for statistical assumptions and concluding with hypothesis testing via multiple regression. This comprehensive analysis aimed to uncover the extent of covariance between risk-taking propensity (and age) with information security compliance behavior.

Assumptions, Limitations, and Delimitations

Acknowledging the study's assumptions about participant honesty and experience with cybercrime was crucial. Limitations stemmed from the cross-sectional data collection method and the purposive sample selection, potentially affecting the internal and external validity of the findings. Delimitations included

focusing on risk propensity and information security behaviors to the exclusion of related concepts like security knowledge and awareness.

Results

This study focused on a group of professional individuals from a single government agency that has implemented strict information security policies. These individuals, selected through Qualtrics, ranged in age from 20 to 60 years and were all required to adhere to their organization's network security guidelines. Aiming for a comprehensive understanding, we set out to engage a minimum of 120 participants, ultimately gathering data from 127 respondents. To better understand the makeup of the sample, the data collected and analyzed included demographic information like age, gender, and the highest level of education attained, using these factors as control variables in the analysis.

The findings, summarized in demographic profiles, reveal that the majority of the participants, nearly 59.1%, identified as male, with females constituting the remaining 40.9%. The age distribution leaned towards older age groups, with the largest segment, 47.24%, falling within the 50-59 age range, and a significant majority, 78.74%, being 40 years or older. This age distribution suggests a mature and experienced participant base. Education levels among participants varied, with a notable 44.1% holding a Graduate degree, highlighting a highly educated sample, whereas only a small fraction, 3.1%, reported having an associate degree as their highest qualification.

Through this demographic exploration, the goal was to present a clear participant profile, underscoring the study's adherence to its mission of enhancing organizational performance and security by integrating human factors with established information security policies. This approach underscores the importance of understanding the diverse backgrounds and characteristics of individuals who interact with and influence the effectiveness of cybersecurity measures within governmental agencies. Table 1 shows the diversity of the population, including the wide range of ages and varying levels of education, with a significant proportion holding bachelor's and graduate degrees. This diverse participant profile is crucial for understanding the different perspectives and experiences that influence the effectiveness of cybersecurity measures within governmental agencies.

Table 1: Profile Characteristics of Participants

	Frequency	Percentage of Sample
Gender		
Female	52	40.90
Male	75	59.10
Age		
20-29	8	6.30
30-39	19	14.96
40-49	40	31.50
50-59	60	47.24
Education		
Some college	19	15.00
Associates	4	3.10
Bachelor	48	37.80
Graduate	56	44.10

Several descriptive statistics were included in the study as evidence of the central tendency, variance, and posterior distribution of the data. Mean was used as a measure of central tendency, standard deviation was used as a measure of variance, and skewness and kurtosis were used to determine posterior distribution.

The data was further examined to obtain further meaning through ratios such as the coefficient of variation based on the mean divided by standard deviation and z-scores for skewness and kurtosis based on skewness and kurtosis when divided by the standard error.

The descriptive results for the RTPS included M = 42.30 and SD = 6.84. The coefficient of variation was evidence of a ratio where standard deviation was 6.84 of the mean. The results for the HAIS-Q included M = 87.03 and SD = 4.02, with a coefficient of variation of 4.62%. The skewness and kurtosis did not appear to violate the generally accepted thresholds for skew or kurtosis. However, the HAIS-Q did appear to present evidence that it was minorly platykurtic. Skewness and kurtosis were examined further to determine whether a significant level of skew or kurtosis existed in the dataset. The z-scores for skewness did not include any evidence of a significant skew as RTPS (z-Skew = 0.20) and HAIS-Q (z-Skew = 0.08) both had z-scores lower than 3.29 (Kim, 2013). The z-scores for kurtosis included similar findings, albeit the z-score for kurtosis was higher for the HAIS-Q scale (z-Kurt = -1.62) than the RTPS scale (z-Kurt = -0.09). These findings were evidence supporting the distribution of data having a level of skewness and kurtosis that was not significant. However, further examination of the data concerning normality was necessary.

Table 2: Descriptive Statistics of Participants

	M	SD	Skew	Kurt
RTPS	**42.30**	**6.84**	**-0.04**	**-0.04**
HAIS-Q	87.03	4.02	-0.02	-0.69

NOTE: *n* = 127.

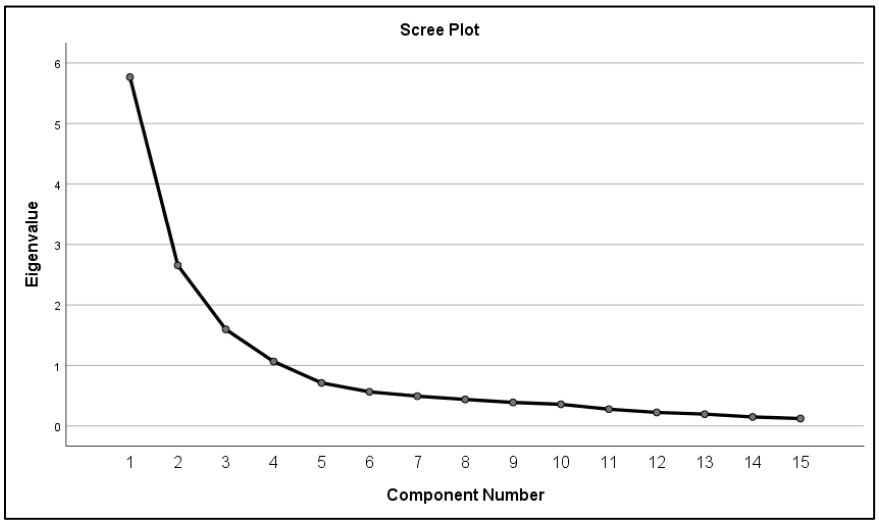

Figure 1: Scree Plot Test

Discussion

RQ1: To what extent does risk-taking propensity covary with information security compliance behavior in a federal agency?

The first research question showed a positive coefficient and demonstrated that government organizations have an interest in ensuring that their workers comply with cybersecurity behavior protocols (Ekran, 2019).

Thus, risk-taking propensity covaries with information security compliance behavior in this federal agency. The information from this first research question demonstrated that risk management is important in federal agencies, based on the relationship between risk-taking propensity to information security compliance in a federal agency. In terms of previous research, the results of the first research question contributed to the research on cybersecurity compliance in a novel way by not supporting extant research and theory. However, most research on RTPS and cybersecurity compliance result in a negative statistical relationship between RTPS and cybersecurity variables (Barlow et al., 2018; Li et al., 2019; McCormac, Zwaans et al., 2017), for research question one, for this study was a positive coefficient. The higher the risk-taking propensity of an individual, the more likely they are to comply with cybersecurity rules and procedures. Accordingly, the result is the opposite direction of effect of previous research as well as of the fundamental proposition of the PMT and the KAB (Parsons et al., 2017). Thus, the implications of the findings show novel information for research via demonstrating that risk-taking propensity covaries with information security compliance behavior in this federal agency. Figure 2 illustrates the relationship between risk-taking propensity and information security compliance behavior in a federal agency, highlighting the positive correlation found in the current study compared to the negative correlations reported in previous research.

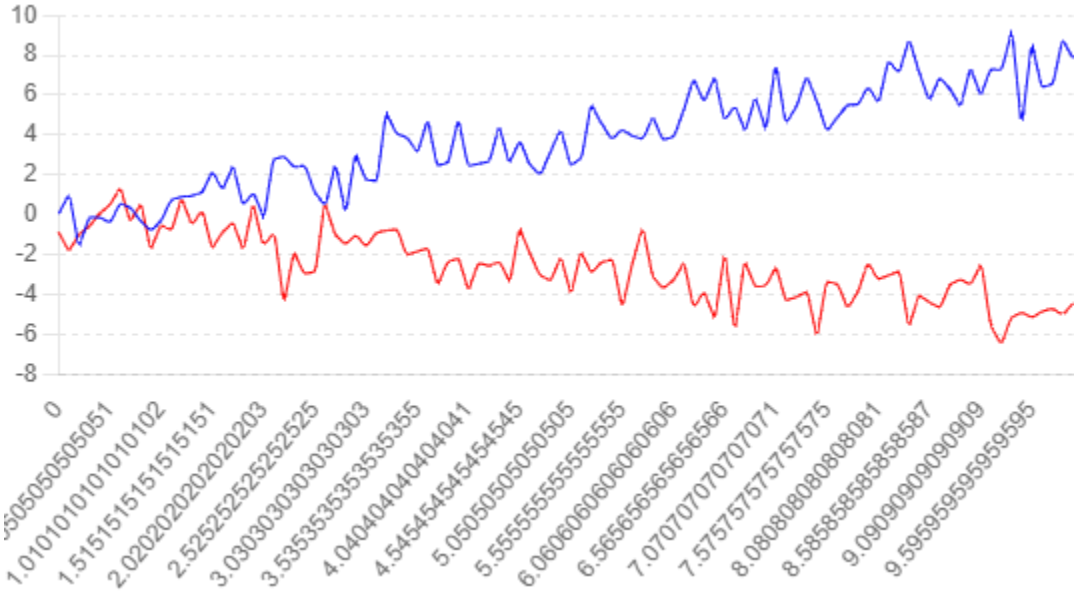

Figure 2: Risk-Taking Propensity vs Information Security Compliance

The implication therefore for both research and theory is that among the examined federal agency, there was a negative statistical relationship with RTPS. The data indicates that there are factors within this agency that potentially result in a negative relationship with cybersecurity compliance and risk-taking propensity. Previous research showed an inverse relationship between risk-taking propensity and cybersecurity compliance (Barlow et al., 2018; Li et al., 2019). Based on these findings, there is a need to examine other factors or attributes within this federal agency. Additionally, future researchers may examine this same agency to confirm the findings of this study and identify actors that may influence the relationship with the RTPS alongside cybersecurity compliance and risk-taking propensity. Furthermore, the result does not falsify extant research and theory on cybersecurity compliance and risk-taking propensity *per se*. Future research is required for exploring the relationship with cybersecurity compliance and risk-taking propensity. However, the findings of this study did show that risk-taking propensity covaries with information security

compliance behavior in this federal agency, which supports the need for practical implementations that address these factors to support outcomes within the agency.

RQ2: To what extent does age covary with information security compliance behavior in a federal agency?

The second research question showed a positive coefficient in both multiple regression analyses with a *p*-value above .05. Age has been associated statistically with low levels of cybersecurity compliance in previous research (Aivazpout & Rao, 2020; Hadlington, 2018; Parsons et al., 2015). Due to the outcome of the finding it is not possible to provide information relevant to the nature of the relationships between age and information security compliance behavior. Numerous studies found a negative and statistically significant relationship between age and cybersecurity compliance variables (Aivazpout & Rao, 2020; Hadlington, 2018; Parsons et al., 2015). Whereas this subset of past research on age and cybersecurity compliance result in a negative and statistically significant relationship (Barlow et al., 2018; Li et al., 2019; McCormac, Zwaans et al., 2017), the results of the second research question for this study was a positive coefficient that was statistically insignificant. However, there are also studies of cybersecurity compliance and age that find no statistically significant relationships between the two variables (Hadlington & Murphy, 2018; McCormac, Zwaans et al., 2017; Wang & Jones, 2020). The research results for the second research question were inconclusive. Figure 3 illustrates the relationship between age and information security compliance behavior in a federal agency. The chart includes both the positive and the negative coefficients from previous research for comparison.

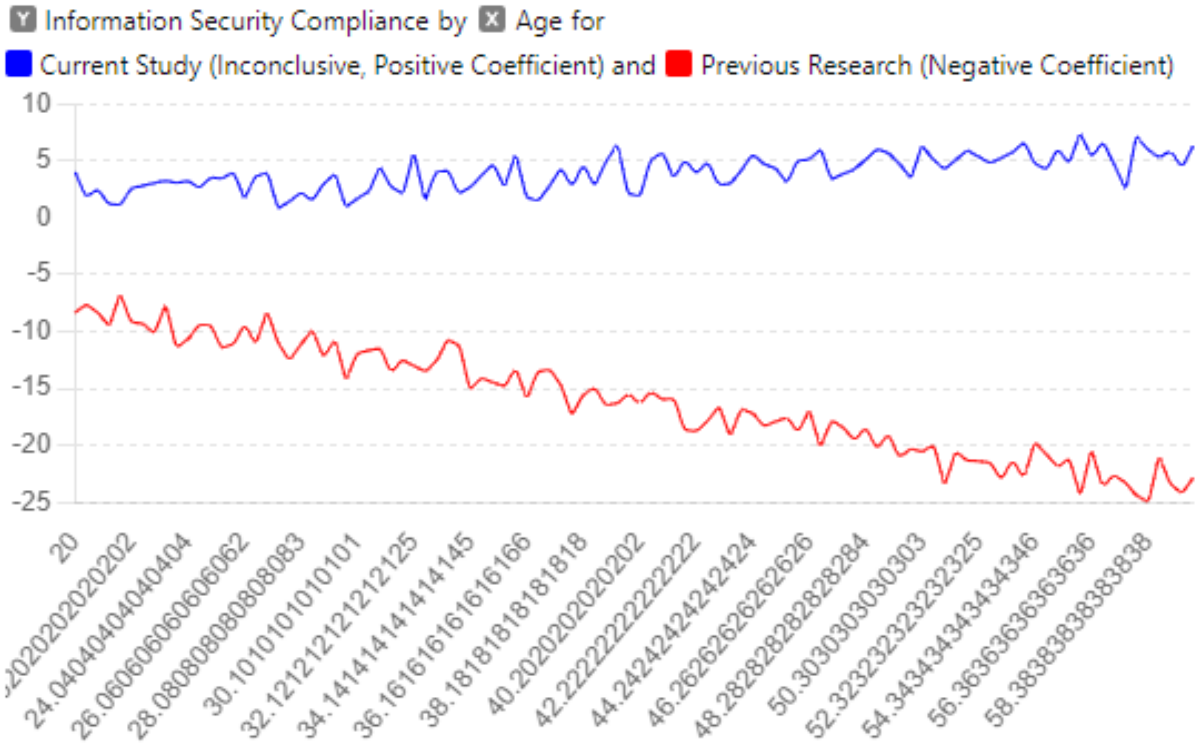

Figure 3: Age vs Information Security Compliance

The implication therefore for both research and theory is that further research on the population of the current study is required which may further demonstrate an improved understanding regarding the factors that potentially mediate the relationship between age and cybersecurity compliance. Because the studies that do not find a statistically significant relationship between cybersecurity compliance and age are not theoretically motivated by theories of generational differences, omitted variable bias may explain when results support the null rather than the alternative hypothesis (Aivazpout & Rao, 2020). The same may be said of the current study. Specifically, when exploring the relationship between PMT or the KAB, it may be important to consider age when examining the relationship with cybersecurity compliance behaviors, perceptions, and attitudes. There is a need to understand the relationship between age and cybersecurity compliance to add further empirical confirmation to previous researcher findings (McCormac, Zwaans et al., 2017; Wang & Jones, 2020).

Recommendations for Practice

Based on the findings, there are several recommendations for practice in the future. The first recommendation for practice is in relationship to research question one and the findings that risk-taking propensity covaries with information security compliance behavior in this federal agency. A recommendation for practitioners would entail the improvement of policies and practices that encourage risk-taking propensity among cybersecurity professionals. Encouraging risk-taking propensity may prove useful for fostering cybersecurity policy compliance.

The second recommendation in alignment with research question one is that strategies should focus on risk-taking propensity as a human factor to be assessed in information security compliance. The results highlight the importance of assessing and mitigating risk-taking propensity within the context of information security compliance. Practitioners wishing to apply the second recommendation may find useful outcomes for ensuring risk taking propensity is an important context within their organization when assessing human factors.

The third recommendation for practice involves the potential use of targeted risk tool assessments and strategies. In alignment with research question one, it may be important to understand risk taking propensity in the context of strategies that are effective for governmental workers. The third recommendation is to identify potential risk factors and implement appropriate control measures to reduce the likelihood of non-compliant behaviors. This should be done to determine the magnitude of risk-taking propensity in the scope of worker behaviors. As the findings of the current research support the existence of a positive relationship between risk-taking propensity and information security compliance, the inclusion of employees that have higher RTSP will increase compliance levels among employees. Thus, risk-taking should be a part of performance evaluation and incentive systems to reinforce compliance with information security protocol.

Recommendations for Future Research

The first recommendation for future research is to explore additional mediating variables as a means of further understanding the factors that affect compliance behavior. The research findings showed a positive statistical relationship between risk-taking propensity and information security compliance. Examining additional mediating variables may include factors related to employee perceptions, other psychological processes, and mediating variables within the organization that contribute to compliance behavior. Other potential moderating variables, such as organizational culture, job roles, or industry sectors, are used to identify whether the strength or direction of the relationship varies based on these contextual factors. Future research is recommended to expand upon this assessment for a means of understanding the ways in which other variables potentially mediate compliance behavior.

The second recommendation for research is to evaluate the potential development of intervention strategies to effectively manage risk-taking propensity and improve information security compliance. Investigating the effectiveness of various interventions, such as training programs, policy changes, or awareness campaigns, would contribute to developing evidence-based practices for promoting compliance behaviors and mitigating the negative effects of risk-taking propensity. Researchers could also employ the same study designs in different worker contexts upon examining potential intervention strategies. Data gathered from such interventional strategy development and evaluation could also potentially support an understanding of the inconclusive findings of age and compliance behavior identified in this study.

Conclusions

In summary, this study examining the correlation between risk-taking propensity and information security compliance among government personnel furnishes compelling empirical support that risk-taking propensity emerges as a robust and statistically significant predictor of information security compliance. These findings underscore the necessity of integrating individual risk profiles into the formulation of interventions and policies aimed at bolstering compliance behaviors. Furthermore, the study's emphasis on government employees accentuates the pertinence of this association within distinct professional milieus.

This empirical contribution augments the burgeoning literature on information security compliance and accentuates the imperative for further scholarly inquiry into mediating mechanisms, moderating factors, longitudinal dynamics, intervention methodologies, and comparative analyses across diverse demographic cohorts. By deepening our comprehension of the intricate interplay between risk-taking propensity and information security compliance, researchers can pave the way for more efficacious practices and policies in safeguarding sensitive information across multifarious organizational landscapes.

The principal takeaway from this investigation manifests as a statistically significant positive association between risk-taking propensity and information security compliance, particularly observable among government personnel. These findings accentuate the importance of discerning individual risk profiles in endeavors aimed at ameliorating compliance behaviors. By acknowledging and mitigating risk-taking proclivities, organizations can cultivate bespoke strategies to fortify information security protocols.

This inquiry underscores the necessity of factoring individual characteristics into the promotion of secure behaviors and lays the groundwork for future interventions and policies tailored to specific vocational settings. Ultimately, prioritizing risk management and acknowledging the ramifications of risk-taking propensity can significantly contribute to the protection of sensitive information within governmental and organizational spheres.

The ramifications of this research hold practical significance, particularly within the domain of information security compliance among government employees. The investigation illuminated a statistically significant positive nexus between risk-taking propensity and compliance behaviors. Subsequent researchers are advised to recognize the pivotal role of individual risk profiles when organizations endeavor to enhance information security practices (Astakhova, 2020; Dalal et al., 2021). To effectively address risk-taking inclinations, organizations should develop targeted strategies that acknowledge and mitigate individual risk profiles (Wang & Jones, 2020). By tailoring interventions and policies to specific vocational contexts, organizations can foster secure behaviors and augment compliance with information security protocols (Rashid & Miri, 2021).

References

Aivazpour, Z. & Rao, V. (2020). Information disclosure and privacy paradox: The role of impulsivity. *Data Base for Advances in Information Security, 51*(1), 14-36. https://doi.org/10.1145/3380799.3380803

Astakhova, L. V. (2020). The validity of information security risk assessment methods for organizations. *Scientific & Technical Information Processing, 47*(4), 241–247.

Barlow, J., Warkentin, M., Ormond, D., & Dennis, A. (2018). Do not even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal of the Association for Information Systems, 19*(8) 689-715. https://doi.org/10.17705/ljais.00506

Dalal, R. S., Bass, A. E., & Aggarwal, V. (2021). Human Factors in Cybersecurity: Integrating Behavioral Insights. Cybersecurity Journal, 5(2), 33-47.

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*. doi: https://doi.org/10.1007/s10869-021-09732-9

Ekran, T. (2019). *Insider threats in the US federal government: Detection and prevention.* Ekran Systems. https://www.ekransystem.com/en/blog/insider-threats-us-federal-government-detection-and-prevention

Hadlington, L. (2018). Employees attitude toward cyber security and risky online behaviors: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. https://doi.org/10.5281/zenodo.1467909.

Hadlington, L. (2018). The Human Factor in Cybersecurity: Exploring the Impact of Employee Behavior on Information Security. Journal of Information Security, 9(3), 189-200.

Khando, A., Li, Q., & Sharma, P. (2021). Economic Implications of Cybersecurity Breaches: A Global Perspective. Economics of Cybersecurity, 12(1), 45-62.

Li, L., He, W., Ash, I., Anwar, M. & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45,* 13-24. Doi: 10.1016/j.ininfomgt.2018.10.017

McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., & Kreuzer, C. (2017). The Role of Individual Differences in Cyber Security Behaviors. Computers & Security, 69, 1-12.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Nasir, M., Arshad, J., & Khurram, M. (2019). Cybersecurity Policies and Practices: Understanding the Human Factor. International Journal of Cybersecurity, 8(4), 240-256.

Parsons, K., Calic, D., Pattinson, M. Butavicius, M., McCormac, A. & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-52. https://doi.org/10.1016/j.cose.2017.01.004

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M. & Jerram, C. (2015). The influence of organizational information security culture on cybersecurity decision making. *Journal of Cognitive engineering and Decision Making: Special Issue on Cybersecurity Decision Making, 9*(2), 117-129. https://doi.org/10.1177/1555343415575152

Rashid, F., & Miri, A. (2021). *User and event behavior analytics on differentially private data for anomaly detection*. 7th IEEE International Conference on Big Data Security on Cloud (pp. 81-86). IEEE. https://doi.org/10.1109/BigDataSecurityHPSCIDS52275.2021.00025

Safa, N. S., Solms, R., & Futcher, L. (2018). Human Aspects of Information Security: A Case Study in Healthcare. Journal of Medical Systems, 42(5), 1-12.

Wang, L., & Jones, R. (2020). Big data analytics in cyber security: Network traffic and attacks. *Journal of Computer Information Systems*, 1-8.