Contents lists available at GrowingScience

Journal of Project Management

homepage: www.GrowingScience.com/jpm

Cybersecurity knowledge and project sustainability: The moderated-moderation effect of perceived risk and risk behavior

Emad Tariq[a*]

[a]*Department of Marketing, Digital Media and MIS, College of Business Administration, Prince Mohammad Bin Fahd University, Al Khobar, Saudi Arabia*

C H R O N I C L E

Article history:
Received January 7, 2026
Received in revised format February 29, 2026
Accepted March 12 2026
Available online March 12 2026

Keywords:
Project Management
Cybersecurity Knowledge
Perceived Threat
Risk of Behavior
Organizational Sustainability
Project Management

A B S T R A C T

Cybersecurity threats have become a structural risk to digital project management, challenging not only digital data integrity but also long-term organizational sustainability. While prior research has emphasized awareness and technical safeguards, limited attention has been given to the behavioral–cognitive mechanisms through which cybersecurity knowledge translates into sustainable organizational outcomes. Drawing on Protection Motivation Theory and the Theory of Planned Behavior, this study examines the moderated-moderation effect of Perceived Risk (PR) and Risk of Behavior (RB) on the relationship between Cybersecurity Knowledge of Threats (CKT) and Organizational Sustainability (OS). Using survey data collected from 235 project management staff across UK organizations, the results of structural equation modeling reveal a significant three-way interaction (CKT × PR × RB). The findings indicate that CKT enhances OS most strongly when both PR and RB are high, suggesting that knowledge translates into sustainability only when employees accurately perceive cyber threats and respond with appropriate protective actions. This joint amplification effect uncovers a previously underexplored mechanism linking individual-level cognition to macro-level organizational resilience.

© 2026 by the authors; licensee Growing Science, Canada.

1. Introduction

The rapid transformation of digital project processes has fundamentally changed how organizations deliver instruction and facilitate e-learning. While these changes have improved efficiency and accessibility, they have also created new vulnerabilities to cyber threats. In recent years, UK organizations have faced a growing wave of sophisticated cyberattacks that threaten their daily operations, financial stability, reputation, and long-term sustainability (NSCS, 2025). The vast amounts of valuable data they store, including intellectual property, project outputs, and staff information, make organizations prime targets for cybercriminals (Ansari & Chenniyampallam, 2026). The World Economic Forum has listed cyber resilience among the top five global risk concerns, underscoring its growing importance across all industries, including project management (WEForum, 2025). Consequently, the relationship between cybersecurity awareness and organizational sustainability has emerged as a critical area of investigation, with major implications for organizational resilience and long-term stability (Harake, 2025).

Within this broader context, it is essential to understand how cybersecurity knowledge can lead to more sustainable organizational practices through the influence of psychological and behavioral factors. Although cybersecurity awareness has improved, the literature reveals significant gaps in understanding the human elements that contribute to an organization's ability to withstand and recover from cyber incidents during projects (Khadka & Ullah, 2025). Scholars argue that IT software alone is insufficient and must be reinforced by human awareness and adaptive behavior (Al Badayneh et al., 2025). Human factors are crucial for enhancing organizational resilience against cyber threats (Triplett, 2022).

Consequently, this study integrates digital contexts with human factors such as perceived risk and risk behavior to examine how they impact the relationship between cybersecurity knowledge of threats and organizational sustainability, thereby addressing a gap in the literature (Ajzen, 2011). The study employs a useful framework for examining how human factors

* Corresponding author
E-mail address etariq@pmu.edu.sa (M. Tariq)

ISSN 2371-8374 (Online) - ISSN 2371-8366 (Print)
© 2026 by the authors; licensee Growing Science, Canada
doi: 10.5267/j.jpm.2026.3.005

influence security-related behaviors (Herath & Rao, 2009; Tariq et al., 2024). By applying theoretical principles, the research integrates cybersecurity knowledge of threats, organizational sustainability, threat perception, and risk behavior into a unified conceptual model. This approach offers a fresh perspective on cybersecurity in projects. This study contributes to the literature by offering a behavioral perspective on how cybersecurity knowledge supports organizational sustainability in project management environments. It demonstrates that cybersecurity knowledge alone is insufficient unless individuals also perceive cyber risks and respond with appropriate behavioral caution. By identifying the interactive role of perceived cyber risk and behavioral risk propensity, the study reveals a previously underexplored mechanism linking individual cognition with organizational resilience. These findings highlight the importance of integrating behavioral awareness and risk interpretation into cybersecurity strategies to strengthen long-term sustainability in organizations.

2. Literature Review

2.1 Cybersecurity and Project Sustainability

Cybersecurity knowledge refers to an organization's understanding of the nature, forms, and potential implications of the cyber risks it encounters (Singh et al., 2025). In contrast, organizational sustainability reflects a project's capacity to ensure continuity and safeguard assets throughout the project lifecycle stages, despite ongoing digital threats (Gündüzyeli, 2025). This conceptualization aligns with broader interpretations of sustainability that emphasize resilience, adaptability, and long-term viability. Researchers posit that cybersecurity resilience has become a decisive factor in sustaining organizations and maintaining greater stakeholder confidence (Bansal & Axelton, 2024). Sustainability increasingly depends on digital resilience, specifically, an organization's ability to defend against, adapt to, and recover from cyber incidents during projects (Sadik et al., 2020; Algremazy, 2023).

Empirical evidence supports a direct association between cybersecurity knowledge of threats and organizational sustainability. For example, studies in Saudi Arabia revealed that cybersecurity systems significantly enhance project performance, particularly when employees possess strong knowledge about system elements (Alotaibi, Alghamdi & Alshamrani, 2024). Similarly, research has shown that organizational resilience depends on how academic communities understand digital risks and apply effective countermeasures (Cremer et al., 2022). Scholars argue that cybersecurity knowledge forms the cognitive foundation of an organization's overall security posture, guiding protective behaviors and informed decision-making (Rotas & Cahapay, 2021; Komissarova & Omar, 2024). Within project-based organizations, such knowledge encompasses awareness of phishing schemes, familiarity with malware threats, recognition of social engineering tactics, and understanding of organizational policies and procedures for maintaining digital security (Al-Janabi, 2024; Lallie et al., 2025). Sustainability in cybersecurity thus extends beyond short-term protection to encompass long-term resilience, regulatory compliance, stakeholder confidence, and operational continuity (Saeed et al., 2023; Sadik et al., 2020). Al-Somali et al. (2024) demonstrated that cybersecurity systems accompanied by strong knowledge and staff engagement contribute directly to sustainable project performance.

2.2 Types of Cyber Threats

Project management institutions face a wide spectrum of cyber threats that differ in intent, sophistication, potential impact, risk, and context (Yao et al., 2025; Algremazy, 2023). Common attacks such as malware, ransomware, software viruses, worms, trojans, and distributed denial-of-service (DDoS) operations can cause extensive operational disruption, significant financial losses, and long-term reputational harm (Sadik et al., 2020). The UK National Cyber Security Centre (NCSC, 2025) has identified phishing as one of the predominant threats affecting project implementation in 2025. By deceiving individuals into disclosing sensitive credentials or performing harmful actions, attackers often circumvent even advanced technical safeguards (Almansoori et al., 2023). This manipulation of human psychology underscores the critical importance of cultivating employee awareness and reinforcing behavioral defenses against social engineering tactics (Saeed et al., 2023).

Ransomware presents another major risk, particularly to organizations that rely heavily on digital infrastructure and sensitive research data. Such attacks encrypt or disable access to organizational systems, disrupting operations and threatening data integrity (Lallie et al., 2025). Insider threat is another challenge, where individuals with legitimate access intentionally or inadvertently compromise security through negligence, error, or misuse of privileges (Almansoori et al., 2023; Akter et al., 2025). Insider threats frequently go unnoticed until substantial damage has already occurred (Maalem Lahcen et al., 2020). Denial-of-Service (DoS) attacks, including their distributed variants, represent another sophisticated category of cyber aggression. These attacks, often attributed to organized or state-sponsored actors, aim to disrupt essential digital services or extract critical organizational data (Mittal, 2024; Maalem Lahcen et al., 2020). Despite the growing prevalence of such incidents, scholars argue that empirical research on cyber threats within project management remains limited, with significant gaps in the literature regarding organizational practices and threat management approaches (Zeb, 2024). The diversity and evolving complexity of cyber threats highlight the necessity of comprehensive cyber threat knowledge among organizational members. Such understanding enables organizations to anticipate, recognize, and effectively mitigate a wide range of digital risks, thereby strengthening their overall cybersecurity resilience and sustainability (Saeed et al., 2023).

2.3 Cybersecurity Knowledge of Threats (CKT)

CKT refers to an organization's understanding of the nature, types, and potential consequences of cyber risks (Singar & Akhilesh, 2019). Possessing this knowledge enhances decision-making, strengthens risk management, and supports proactive defense strategies (Almansoori et al., 2023). Academics have demonstrated that cybersecurity knowledge of threats can be influenced by perceived risk and protective behavior (Saeed et al., 2023; Mittal, 2024). Kennedy and Chan-Tin (2020), for instance, observed that cybersecurity knowledge is significantly influenced by perceptions of cyber threats. Likewise, Chee Keong et al. (2025) found that small and medium-sized enterprises (SMEs) with stronger situational cybersecurity awareness achieve greater long-term sustainability. In the context of project management, CKT extends beyond technical understanding to encompass the ability to recognize cyber threats (Ansari & Chenniyampallam, 2026). Recent studies have affirmed that CKT is a fundamental component of an organization's overall security posture, serving as the cognitive basis for informed decision-making and protective behaviors among employees (Saeed et al., 2023; Lallie et al., 2025). The link between CKT and organizational sustainability has been highlighted in empirical studies. Research on Saudi Arabian SMEs indicates that robust cybersecurity systems, underpinned by strong knowledge frameworks, significantly enhance sustainable business performance (Alotaibi, Alghamdi & Alshamrani, 2024). Similarly, research on the digital transformation of projects suggests that organizational resilience is partly determined by the community's collective understanding of digital threats and their capacity to implement effective countermeasures (Cremer et al., 2022). These findings collectively imply that cyber threat knowledge contributes to sustainability by fostering proactive threat identification, encouraging compliant and proactive behavior, and facilitating rapid organizational response to security incidents.

2.4 Perceived Risk (PR): A Moderator Effect

Perceived Risk (PR) refers to an individual's subjective evaluation of potential threats and their severity, which plays a crucial role in motivating protective behavior (Raz et al., 2002). The Technology Threat Avoidance Theory (TTAT) considers PR a vital construct that determines whether technology-related threats are effectively transformed into preventive or defensive action (Liang, Yajiong & Xue, 2009; Alsmadi et al., 2022). Scholars have proposed that perceived cyber threats may influence the relationship between knowledge and behavioral outcomes; however, empirical evidence within cybersecurity contexts remains limited (Naw & Kohsuwan, 2023). When PR is low, individuals may fail to recognize the urgency of applying their knowledge, leading to inaction. Conversely, individuals who perceive higher levels of cyber risk are more likely to act upon their knowledge, adopting proactive security behaviors that contribute to both organizational resilience and sustainability (Zainal et al., 2021; Akter et al., 2025). Therefore, the moderating role of PR can strengthen the significance of CKT, amplifying its impact on organizational sustainability.

2.5 Risk of Behavior (RB): A Moderated-Moderation Perspective

Risk of Behavior (RB) refers to the consistent and deliberate actions individuals take in response to potential risks (Snider, Shandler & Zandani, 2021). The Protection Motivation Theory (PMT) explains how individuals are motivated to protect themselves from perceived threats through cognitive behavioral processes (Rogers & Ronald, 1975). Scholars argue that behavioral responses to risk can strengthen the relationship between Cybersecurity Knowledge of Threats (CKT) and organizational sustainability by translating knowledge into practical security actions (Araujo, Machado & Passos, 2024). In this sense, behavior serves as the moderator linking CKT and Organizational Sustainability (OS) (Wolff, Mann & Koppen, 2024). Saeed (2023) found that employees with higher behavioral engagement, such as creating strong passwords or promptly reporting phishing attempts, significantly reduce organizational vulnerability. Qalby et al. (2024) observed that organizations encouraging proactive Risk of Behavior (RB) demonstrated greater resilience to cyberattacks by their employees.

In addition, the Theory of Planned Behavior (TPB) provides the psychological foundation for the moderated-moderation model by explaining that knowledge alone does not ensure risk-mitigating behavior; rather, perceived risk interacts with knowledge to shape cybersecurity practices that enhance organizational sustainability (Ajzen, 1991). In the cybersecurity context, recent studies have proposed that PR can moderate the influence of CKT on RB; however, this effect appears most significant when PR is high (Naw & Kohsuwan, 2023). Philip, Herrmann, and Hampel (2024) argued that PR alone cannot guarantee positive RB unless individuals perceive the risk as both real and personal. Almansoori et al. (2023) confirmed that employees with heightened PR were more motivated to engage in defensive actions as RB. Consequently, the interaction among CKT, PR, and RB may therefore play a critical role in shaping Organizational Sustainability (OS). This three-way interaction supports the theoretical rationale that CKT, PR, and RB must jointly translate into tangible action to achieve sustainable cybersecurity performance.

3. Conceptual Gap

Although dyadic relationships between CKT and RB, and between PR and RB, have been widely examined, empirical investigations involving dual moderation effects remain scarce (Hair et al., 2019; Maalem Lahcen et al., 2020). Academics posit that most cybersecurity behavior models continue to rely on linear or single-moderator frameworks, which fail to capture the complex interdependencies among multiple cognitive and behavioral constructs (Almansoori, Al Emran & Shaalan, 2023). Maalem Lahcen et al. (2020, p. 9) claimed that "there is a gap in the application of advanced modelling techniques that consider the complex interdependence among multiple predictors and moderators." Furthermore, both academic literature

and government reports have highlighted the scarcity of research on cybersecurity risk and resilience within project management (Zeb, 2024; Algremazy, 2023). In other words, there is a lack of research exploring the moderated-moderation effect of PR and RB on the CKT–OS relationship. Consequently, this study aims to measure the interactive moderated-moderation effect of PR and RB on the relationship between CKT and OS, thereby contributing to two theoretical frameworks and addressing a gap in the literature.

4. Research Questions and Hypotheses

Drawing upon the reviewed literature, the study proposes the following research questions:

RQ1: Does Cybersecurity Knowledge of Threats (CKT) have a direct influence on Organizational Sustainability (OS)?

RQ2: Does Perceived Risk (PR) moderate the relationship between CKT and OS?

RQ3: Does Risk of Behavior (RB) moderate the relationship between CKT and OS?

RQ4: Does the full moderated-moderation interaction between PR and RB strengthen the effect of CKT on OS?

The research hypotheses are as follows:

H_1: *CKT has a significant direct positive effect on OS.*

H_2: *PR has a significant positive moderating effect on the relationship between CKT and OS.*

H_3: *RB has a significant positive moderating effect on the relationship between CKT and OS.*

H_4: *The interaction effect of PR with RB has a strong and significant positive moderating effect on the relationship between CKT and OS.*

5. Methodology

This study employed a quantitative research approach, utilizing an online questionnaire to examine the effect of Cybersecurity Knowledge of Threats (CKT) on Organizational Sustainability (OS) with the moderated-moderation effect of Perceived Risk (PR) and Risk of Behavior (RB), both independently and interactively. The quantitative approach is appropriate as it ensures statistical testing of complex relationships and supports the generalization of results (Creswell & Creswell, 2018). Online surveys were used as an effective data collection method due to their efficiency, cost-effectiveness, and ability to reach a wide and diverse population of respondents (Evans & Mathur, 2005).

A random sampling method was used to target participants from multiple organizations across the United Kingdom, encompassing both academic and administrative staff. This sampling technique was selected to minimize bias and enhance the representativeness of the findings (Acharya, Prakash, Saxena, & Nigam, 2013). Random sampling ensured that each potential participant had an equal probability of selection, improving the reliability and external validity of the statistical outcomes (Taherdoost, 2016). A total of 300 email invitations were distributed through organizational mailing lists. Participants were provided with an online questionnaire containing items measured on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Participation was voluntary, and respondents were briefed on the study's aims, scope, and confidentiality measures through an informed consent form presented before the survey. Data collection spanned four weeks, with reminder emails sent after two weeks to improve response rates. Following a rigorous screening and data-cleaning process to remove incomplete or duplicate entries (Cunningham & Muir, 2023), 235 valid responses were retained, exceeding the minimum threshold recommended for SEM analyses involving interaction effects (Kline, 2016).

Ethical compliance was strictly maintained in accordance with organizational guidelines and professional standards. The study obtained formal approval from the organizational ethics committee before data collection. Anonymity and confidentiality were guaranteed by avoiding the collection of identifying details. These procedures align with the ethical principles of the British Psychological Society (BPS, 2021) and the General Data Protection Regulation (GDPR, 2018). The survey instrument was adopted from previously validated scales to ensure conceptual accuracy and reliability.

6. Analysis Results and Findings

Data were analyzed using Structural Equation Modelling (SEM) with STATA 17, as SEM allows for the simultaneous estimation of multiple relationships among latent variables, including moderation and interaction effects (Sardeshmukh & Vandenberg, 2017). The measurement model was first validated through Confirmatory Factor Analysis (CFA) to assess construct reliability and validity (Brown, 2015; Browne & Cudeck, 1993; Fornell & Larcker, 1981). Prior to CFA, data suitability was confirmed using the Kaiser–Meyer–Olkin (KMO) measure (Kaiser, 1974) and Bartlett's Test of Sphericity (Field, 2018; Byrne, 2016). Results indicated that the data were appropriate for factor analysis (KMO = 0.735; Bartlett's $\chi^2(102) = 1038.52$, $p < 0.001$), confirming adequate sampling and significant intercorrelations among items. The Average Variance Extracted (AVE) values for all constructs (CKT, PR, RB, and OS) exceeded 0.50, confirming convergent validity. The study further tested the hypothesized interaction effects of PR and RB, both independently and jointly, on the relationship

between CKT and OS. Across the 235 valid responses, sample analysis indicated that 87.2% of participants possessed over two years of experience in project management, suggesting a high level of contextual familiarity with cybersecurity systems and practices (see table below). This demographic distribution strengthened the credibility of the findings and the contextual relevance of the proposed moderated-moderation model.

Table 1
Sample Analysis

Variable & category	N	%
Gender status		
Male	85	36.2
Female	150	63.8
Education level		
University	57	24.3
Master	93	39.6
PhD	81	34.5
Other	4	1.7
Current job position		
Administration or Finance (Staff)	102	43.4
Academic	133	56.6
Experience in this sector		
Less than 1 year	30	12.8
2–5 years	75	31.9
6–10 years	43	18.3
11–15 years	45	19.1
More than 16 years	42	17.9

6.1 Direct Effects

As shown in Table 5, CKT has a reliable and positive relationship with OS (β = 0.25, CR = 1.56, p = .02), emphasizing that employees' knowledge of cyber threats is an important driver of organizational sustainability. These findings confirm scholars' arguments that knowledge of cyber threats supports adherence to security policies and maintains operational continuity, thereby reinforcing sustainable organizational practices (Alotaibi et al., 2024; Saeed et al., 2023).

6.2 Single Moderating Effects

This research tested the individual moderating effects of Perceived Risk (PR) and Risk of Behavior (RB) on the relationship between CKT and OS. The interaction between CKT and PR was reliable, positive, and highly significant (β = 0.68, CR = 4.06, p < .001), suggesting that the impact of cyber threat knowledge on sustainability is strengthened when employees perceive cyber risks as serious. These results are consistent with the Protection Motivation Theory (PMT), which posits that the salience of a threat motivates individuals to act on their knowledge (Herath & Rao, 2009). Conversely, the interaction between CKT and RB showed a weak positive effect (β = 0.21, CR = 0.83, p = .05), indicating that behavior alone is not a sufficient amplifier of knowledge's effect on OS. This finding emphasizes that actions must be supported by Risk Perception (RP). However, the interaction between PR and RB was both strong, reliable, and highly significant (β = 0.57, CR = 4.84, p < .001). These results support the findings that individuals' behaviors toward cybersecurity risks depend on how they perceive those risks, as well as their motivations or situational context (Vance et al., 2014; Aurigemma & Mattson, 2017; Han et al., 2025).

6.3 Full Moderated-Moderation Effect

This step aligned with prior findings that cognitive awareness must be coupled with appropriate motivation and action to achieve meaningful outcomes in cybersecurity contexts (Almansoori et al., 2023; Philip, Herrmann & Hampel, 2024; Han et al., 2025). Consequently, this study tested the three-variable interaction (CKT × PR × RB), and the results indicated a statistically significant, positive, and reliable interaction effect (β = 0.17, CR = 2.29, p < .001). This provides strong evidence for a full and robust moderated-moderation effect, indicating that PR and RB together create a synergistic effect on OS, which in turn contributes to potential organizational success. This interaction suggests that the alignment or joint influence of PR and RB is particularly powerful in shaping positive organizational sustainability. The relationship is statistically significant and unlikely to be due to chance. Table 2 illustrates the moderation effects among CKT, PR, RB, and OS.

Table 2
Direct Effect, Single Moderator Effect, and Full Moderation Effect

	Std. Est. (β)	SE	CR (z)	p-value	Sig.
CKT → OS	0.25	0.16	1.56	.02	**
CKT × PR → OS	0.68	0.17	4.06	< .001	***
CKT × RB → OS	0.21	0.25	0.83	.05	**
PR × RB → OS	0.57	0.12	4.84	< .001	***
CKT × PR × RB → OS	0.17	0.13	2.29	< .001	***

Note: Significance levels are indicated as follows: ***p < .01, **p < .05, *p < .1

Fig. 1 shows the moderation effect between CKT, PR, RB and OS

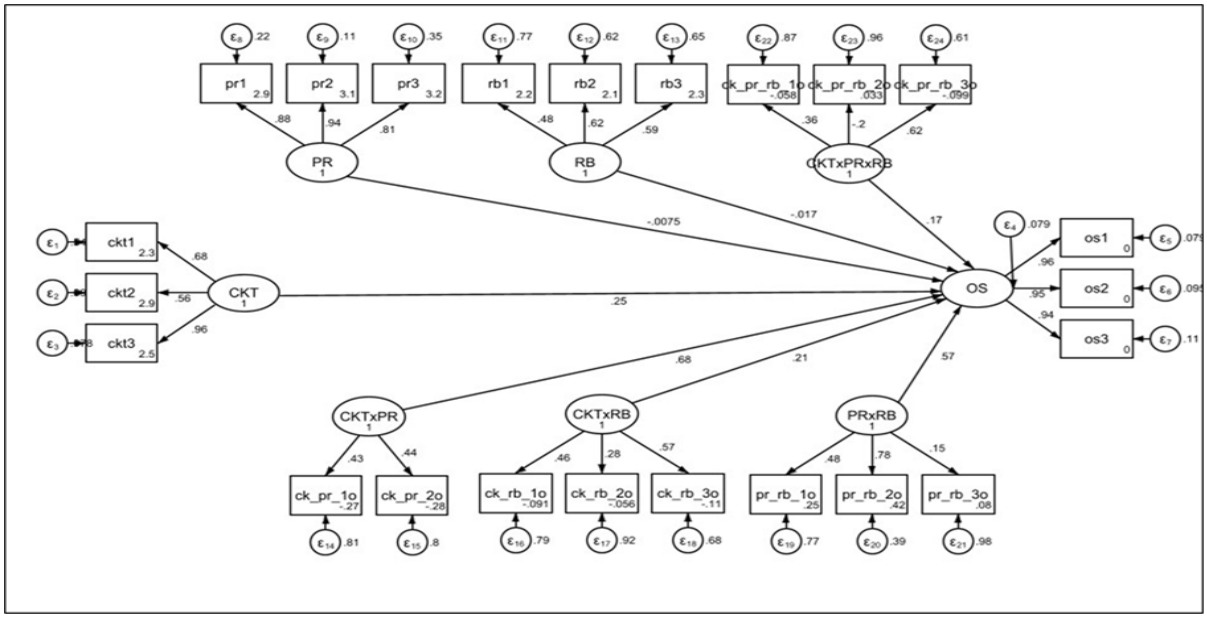

Fig. 1. The moderation effect between CKT, PR, RB and OS

Consequently, the results show that PR plays an important role in shaping how CKT influences OS. Specifically, the strong two-way interaction between CKT and PR ($\beta = .68$, $p < .001$) indicates that when PR is higher, the positive impact of CKT on OS becomes substantially stronger. The significant three-way interaction among CKT, PR, and RB ($\beta = .17$, $p < .001$) further suggests that this pattern depends on RB. In other words, the effect of PR on the CKT–OS relationship is not uniform across all levels of RB; it becomes especially pronounced when RB is also high. Although the three-way effect is smaller in magnitude, it reveals a more meaningful dynamic among the three factors. In practice, this suggests that organizational sustainability depends not only on knowledge acquisition but also on aligning perception and action in a coherent, proactive manner.

7. Discussion

The results indicate that Cyber Threat Knowledge (CKT) has a positive and significant relationship with Organizational Sustainability (OS). This finding suggests that employees' understanding of cyber threats contributes meaningfully to the sustainability of organizational operations. When employees are knowledgeable about cybersecurity risks, they are more likely to follow security policies, recognize potential vulnerabilities, and adopt practices that protect digital infrastructures. These behaviors help organizations maintain operational continuity and reduce disruptions caused by cyber incidents. The findings support previous studies that emphasize the role of cybersecurity knowledge in promoting responsible security behavior and strengthening sustainable organizational practices (Alotaibi et al., 2024; Saeed et al., 2023).

This study also examined whether Perceived Risk (PR) and Risk Behavior (RB) influence the relationship between cyber threat knowledge and organizational sustainability. The results show that PR significantly strengthens the effect of CKT on OS. In other words, when employees perceive cyber threats as serious and potentially harmful, their knowledge becomes more effective in supporting sustainable organizational outcomes. This finding aligns with Protection Motivation Theory (PMT), which suggests that individuals are more likely to act on their knowledge when they perceive a threat as significant (Herath & Rao, 2009). In contrast, the moderating effect of RB on the relationship between CKT and OS was weaker. This indicates that behavioral responses alone may not be sufficient to strengthen the impact of cybersecurity knowledge. Instead, behavior appears to be more meaningful when accompanied by a strong perception of cyber risk. However, the interaction between PR and RB was both strong and statistically significant, suggesting that employees' cybersecurity behaviors are largely shaped by how they interpret and perceive cyber risks. This finding is consistent with prior research showing that individuals' responses to cybersecurity threats depend on both risk perception and situational motivations (Vance et al., 2014; Aurigemma & Mattson, 2017; Han et al., 2025).

Finally, the study tested a three-way interaction between CKT, PR, and RB, revealing a significant moderated-moderation effect. This result suggests that the relationship between cybersecurity knowledge and organizational sustainability becomes strongest when both perceived risk and behavioral sensitivity to risk are high. In other words, sustainability outcomes are enhanced when employees not only possess cybersecurity knowledge but also accurately perceive cyber threats and respond with appropriate behaviors. These findings reinforce previous research indicating that cognitive awareness alone is

insufficient to achieve effective cybersecurity outcomes. Instead, knowledge must be supported by appropriate motivation and behavioral action (Almansoori et al., 2023; Philip, Herrmann, & Hampel, 2024; Han et al., 2025). The significant three-way interaction highlights a dynamic relationship among knowledge, perception, and behavior in shaping organizational sustainability. Although the magnitude of the three-way effect is smaller than the two-way interaction, it reveals a more nuanced mechanism through which cybersecurity practices contribute to long-term organizational resilience. Overall, the results demonstrate that organizational sustainability in cybersecurity contexts depends not only on developing employee knowledge but also on fostering accurate risk perception and responsible behavioral responses. When these elements are aligned, organizations are better positioned to build resilient and sustainable cybersecurity practices.

8. Conclusion

This study investigated how Cybersecurity Knowledge of Threats (CKT) influences Organizational Sustainability (OS) in digital project management, considering the moderating roles of Perceived Risk (PR) and Risk of Behavior (RB). The results reveal that perceived risk and risk behavior exert a strong, positive moderated-moderation interaction effect on the relationship between cybersecurity knowledge of threats and organizational sustainability. This study contributes to the literature in several ways. First, it examines a complex moderated-moderation interaction effect, drawing on the Theory of Planned Behavior (TPB) through the integration of psychological and behavioral factors in a digital structural context (Ajzen, 2011). In other words, the significant three-way interaction (CKT × PR × RB) highlights that alignment among knowledge, risk perception, and behavior is essential for translating cognitive awareness into sustainable organizational outcomes. Second, the research emphasizes the vital role of perceived risk in motivating protective actions and behavior, supporting PMT's propositions in an organizational context (Rogers, 1975). Third, the study addresses a notable gap in the literature: prior research on cybersecurity behavior in project management has largely relied on linear or single-moderator frameworks and has neglected the interactive effect among knowledge, perception, and behavior in influencing organizational sustainability.

9. Limitations and Recommendations

The findings are based on data collected from a specific sample of project management institutions in the UK, which may limit the generalizability of the results. Therefore, future studies should replicate this model across different populations, industries, or cultural contexts to confirm whether the relationships among CKT, PR, RB, and OS hold more broadly. In addition, because the study used cross-sectional data, the relationships identified are correlational rather than causal. Longitudinal or experimental research would be required to establish causal links between CKT, PR, RB, and OS.

The findings offer several insights aimed at strengthening sustainability for project management organizations in the UK. Organizations should incentivize and normalize secure behaviors, such as reporting suspicious emails, updating passwords, and adhering to organizational cybersecurity protocols. Aligning individual actions with organizational objectives ensures that knowledge and perception translate into effective outcomes during projects. Regular assessments of employee knowledge, risk perception, and behavioral engagement can identify gaps and guide targeted interventions.

10. Theoretical Implications

This study contributes to the literature by empirically demonstrating a complex moderated-moderation framework in the context of cybersecurity knowledge and project sustainability. While previous studies have focused on linear or single-moderator models (Maalem Lahcen et al., 2020; Almansoori, Al Emran & Shaalan, 2023), these findings underscore the importance of considering how knowledge, risk perception, and behavior interdependently shape sustainable outcomes.

11. Practical Implications

Academics and government reports have highlighted the scarcity of research on cybersecurity risk and sustainability within project management (Zeb, 2024; NCSC, 2025). For project management organizations in the UK, these results highlight the need for comprehensive cybersecurity programs that integrate knowledge enhancement, risk awareness, and behavioral reinforcement. Training programs should educate staff on identifying and assessing threats, promote an accurate perception of risks without inducing undue fear, and encourage consistent protective behaviors. Policies should align individual actions with organizational objectives to maximize sustainability and resilience.

Acknowledgements

The author would like to express sincere appreciation to all individuals who contributed to the completion of this research. In particular, we extend our gratitude to the staff members across the participating organizations in the United Kingdom who generously shared their time and insights by participating in the survey. Their valuable responses were essential in enabling

the empirical analysis of this study. The author also acknowledges the constructive feedback provided by colleagues and reviewers, whose comments helped improve the clarity and quality of this research. Finally, we appreciate the organizational support that facilitated the development and completion of this study on cybersecurity knowledge and project sustainability.

References

Acharya, A. S., Prakash, A., Saxena, P., & Nigam, A. (2013). Sampling: Why and how of it? *Indian Journal of Medical Specialities, 4*(2), 330–333.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Ajzen, I. (2011). The theory of planned Behavior: Reactions and reflections. *Psychology & Health, 26*(9), 1113–1127.

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J., Thomas, M. K., & Hossain, M. A. (2025). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research, 350*, 673–698.

Al Badayneh, D. M., Al Badayneh, D. D., & Hashish, R. K. (2025). Human factors of cybersecurity. *Journal of Posthumanism, 5*(4), 1302–1314.

Algremazy, N. A., Ideris, Z., Alferjany, M. A., & Akram, A. (2023). The effect of risk management practices on project performance. *International Journal of Professional Business Review, 8*(6), 1–20.

Al-Janabi, S. (2024). Cybersecurity transformation: Cyber-resilient IT project management framework. *Computers, 4*(4).

Almansoori, A., Al-Emran, M., & Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. *Applied Sciences, 13*(9), Article 5700.

Alotaibi, M., Alghamdi, S., & Alshamrani, M. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability, 16*(5), Article 1880.

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: Awareness in COVID-19 age. *Kybernetes, 51*(1), 451–466.

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of SMEs in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability, 16*(5), Article 1880.

Ansari, M. S., & Chenniyampallam, U. R. (2026). Cybersecurity risk management in IT projects: A systematic review and classification of risks, best practices, and framework effectiveness (2020–2025). *SSRN*.

Araujo, M. S., Machado, B. A. S., & Passos, F. U. (2024). Resilience in the context of cyber security: A review of the fundamental concepts and relevance. *Applied Sciences, 14*(5), Article 2116.

Aurigemma, S., & Mattson, T. (2017). Do it for the game: A gamer's perspective on information security behaviors. *Computers & Security, 65*, 376–389.

Bansal, G., & Axelton, Z. (2024). Impact of cybersecurity disclosures on stakeholder intentions. *Journal of Computer Information Systems, 64*(1), 78–91.

Bartlett, M. S. (1954). A note on the multiplying factors for various chi-square approximations. *Journal of the Royal Statistical Society: Series B (Methodological), 16*(2), 296–298.

British Psychological Society. (2021). *BPS code of human research ethics* (4th ed.). https://www.bps.org.uk/news-and-policy/bps-code-human-research-ethics-2nd-edition

Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd ed.). The Guilford Press.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. In K. A. Bollen & J. S. Long (Eds.), *Testing structural equation models* (pp. 136–162). Sage.

Byrne, B. M. (2016). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (3rd ed.). Routledge.

Chee Keong, T., Khan, S. K., & Khattak, U. F. (2025). Exploration of the impact of cyber situational awareness on small and medium enterprises (SMEs) in Malaysia. *Journal of Informatics and Web Engineering, 4*(1), 292–306.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance*.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Cunningham, S. A., & Muir, J. A. (2023). Data cleaning. In A. L. Nichols & J. Edlund (Eds.), *The Cambridge handbook of research methods and statistics for the social and behavioral sciences* (Vol. 1, pp. 443–467). Cambridge University Press.

Evans, J. R., & Mathur, A. (2005). The value of online surveys. *Internet Research, 15*(2), 195–219.

Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5th ed.). SAGE Publications.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50.

General Data Protection Regulation. (2018). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://gdpr.eu/

Gündüzyeli, B. (2025). Cyber resilience in digital marketing within the framework of sustainable management. *Sustainability, 17*(5), Article 2080.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among staff based on protection motivation theory: Evidence from China. *Frontiers in Public Health, 13*, Article 1677024.

Harake, M. F. (2025). Integrating cybersecurity into project management. *PM World Journal, 14*(1).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39*(1), 31–36.

Kennedy, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology, 11*, Article 546546.

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*(3), 1–13.

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). Guilford Press.

Komissarova, A., & Omar, S. (2024, April 18). From threat response to responsibility: Here's how cybersecurity is linked to sustainability. *Forbes Middle East*. https://www.pwc.com/m1/en/media-centre/articles/from-threat-response-to-responsibility-here-is-how-cybersecurity-is-linked-to-sustainability.html

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), Article 49.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71–90.

Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., et al. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(1).

Mittal, C. (2024). An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks. *International Journal of Scientific Research and Management, 12*(4).

National Cyber Security Centre (NCSC). (2025).

Naw, T., & Kohsuwan, P. (2023). Roles of perceived knowledge, risk, and trust in cybersecurity solution implementation: A study in Bangkok, Thailand. *Human Behavior, Development and Society, 24*(3), 1–15.

Philip, N., Herrmann, M., & Hampel, S. (2024). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Article e20963.

Qalby, H., Hariyanto, G. Y., Utomo, D. T., & Rahim, R. K. (2024). The influence of cybersecurity protection behavior: Employees of Big Four account firm companies. *Jurnal Impresi Indonesia, 4*(5), 6684.

Raz, T., Shenhar, A. J., & Dvir, D. (2002). Risk management, project success, and technological uncertainty. *R&D Management, 32*(2), 101–109.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93–114.

Rotas, E., & Cahapay, M. (2021). Does threat knowledge influence protective behaviors of projects in the context of cyber security in digital projects in COVID-19 crisis? *Journal of Pedagogical Sociology and Psychology, 3*(1), 45–53.

Sadik, S., Ahmed, M., Sikos, L. F., & Islam, A. K. M. N. (2020). Toward a sustainable cybersecurity ecosystem. *Computers, 9*(3), Article 74.

Saeed, S. (2023). Digital workplaces and information security behavior of business employees: An empirical study of Saudi Arabia. *Sustainability, 15*(7), Article 6019.

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), Article 7273. https://doi.org/10.3390/s23167273

Sardeshmukh, S. R., & Vandenberg, R. J. (2017). Integrating moderation and mediation: A structural equation modeling approach. *Organizational Research Methods, 20*(4), 721–745.

Singar, A. V., & Akhilesh, K. B. (2019). Role of cyber-security in higher education. In *Smart Technologies: Scope and Applications* (pp. 249–264). Springer.

Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation, 143*, 10–19.

Snider, K. L. G., Shandler, R., & Zandani, S. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity, 7*(1), 1–19.

Taherdoost, H. (2016). Sampling methods in research methodology; How to choose a sampling technique for research. *International Journal of Academic Research in Management, 5*(2), 18–27.

Tariq, E., Akour, I., Al-Shanableh, N., Alquqa, E. K., Alzboun, N., Al-Hawary, S. I. S., & Alshurideh, M. T. (2024). How cybersecurity influences fraud prevention: An empirical study on Jordanian commercial banks. *International Journal of Data and Network Science, 8*(1), 69–76.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy, 2*(3), 573–586.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG). *Journal of the Association for Information Systems, 15*(10), 679–722.

Wolff Mann, E., & Koppen, J. (2024). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*.

World Economic Forum. (2025). *Global Cybersecurity Outlook 2025: Understanding complexity in cyberspace*. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/in-full/1-understanding-complexity-in-cyberspace-587e8c5eba/

Yao, D., De Soto, B. G., & Wilkes, M. (2025). Identifying cyber risk factors associated with construction projects. *Journal of Civil Engineering and Management*, *31*(8), 926-954.

Zainal, N. C., Mohd Puad, M. H., & Mohd Sani, N. F. (2021). Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness. *Asian Social Science, 18*(1), 55–66.

Zeb, S. (2024). *Evaluate the impact of risk management practices on project performance: A case study of the UK construction industry* [Unpublished manuscript]. University of Sunderland.

© 2026 by the authors; licensee Growing Science, Canada. This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (http://creativecommons.org/licenses/by/4.0/).