KASBIT BUSINESS JOURNAL

Journal homepage: www.kbj.kasbit.edu.pk

Human Factor and Cyber Security: Discovering the Correlation between Security Attitudes and Behavioral Intentions to Perform Security linked Behaviors

Dr. Sana Arz Bhutto[i], Dr. Muhammad Imran Khan[ii] & Dr. Sobia Iqbal[iii]

i) *Dean/ Director ORIC, Business Administration Department, Sindh Institute of Management and Technology, Karachi.*

ii) *Assistant Professor, Business Administration Department, Shaheed Zulfiqar Ali Bhutto University of Law*

iii) *Associate Professor, Head of Management Sciences Department, DHA Suffa University, Karachi.*

ARTICLE INFO

Keywords:
Human factors, Cyber security, Perceived vulnerability, Perceived benefits, Pakistan, Banking sector.

ABSTRACT

The study investigates the relationship between human factors, specifically perceived vulnerability and perceived benefits, and security attitudes and behaviors in the banking sector of Pakistan. Using a quantitative approach, data were collected from 150 employees through validated questionnaires. Key findings indicate that perceived vulnerability and perceived benefits significantly influence attitudes toward cyber security, which in turn impact behavioral intentions. Notably, perceived benefits had a stronger effect on attitudes. The study highlights a gap between positive attitudes and actual security behaviors, largely due to organizational culture. Limitations include the focus on a single sector and the cross-sectional design. Future research should consider longitudinal studies and explore other industries for broader applicability. The findings provide practical insights for enhancing cyber security training and policy-making in developing countries.

Corresponding Authors: Dr. Sana Arz Bhutto
Email: arzsana@yahoo.com

Received: 19th August, 2024
Received in revised form: 9th October, 2024
Accepted: 14th November, 2024

The material presented by the authors does not necessarily represent the viewpoint of the editor(s) and the management of the Khadim Ali Shah Bukhari Institute of Technology (KASBIT) as well as the authors' institute © KBJ is published by the Khadim Ali Shah Bukhari Institute of Technology (KASBIT) 84-B, S.M.C.H.S, off Sharah-e-Faisal, Karachi- 74400, Pakistan

1. Introduction

In today’s dynamic context, when the world is transferring to digital forms of business, security has become a significant issue for organizations and personal users. As can be observed, the defensive structure against cyber threats has been considerably strengthened by technological improvements, but one cannot ignore the human factor as an important component of cyber security. The human aspect of cyber security is related to individuals’ actions, beliefs, and perceptions regarding security and the implementation of security standards. Understanding the risks in these human-centric factors is imperative for the formulation of countermeasures to cyber threats and for generally improving the security status of organizations.

As far as the human factor is concerned, people’s activity constitutes potential threats in most cases, as the weakest link is always a human. This is especially important for Pakistan, which is experiencing rapid digitalization and increasingly frequent cyber threats. Despite the use of technology, security malfunctions often originate from actions people take, such as poor password creation, vulnerability to scams, and failure to observe security measures (Ahmad, 2021). Therefore, understanding and guiding people’s perceptions regarding cyber security becomes critical for enhancing security from cyber threats in Pakistan. Pakistan’s banking sector, in particular, has to deal with numerous cyber security issues. The use of online platforms has enhanced banking processes, thus increasing the need for better protection from hackers and other related criminals. However, the execution of these measures still largely depends on the human aspect.

Over the recent past, the banking sector in Pakistan has adopted digital technologies in most of its operations, which has increased its exposure to various cyber threats. However, the specific research gaps this study addresses needs more emphasis. Prior studies mainly focus on technological factors in cyber security, neglecting the psychological and behavioural dimensions, particularly in developing countries. Ali et al. (2023) noted that cyber threats against Pakistani banking organizations have increased, highlighting the need for stronger protection measures. They also observed that Pakistan lacks a highly developed cyber security system and that there are many deficiencies in legislative measures to minimize these threats.

Human factors are critical when it comes to the efficiency of cyber security strategies. The importance of studying cyber security attitudes and behaviours in developing countries like Pakistan is crucial for addressing unique challenges posed by culture, socioeconomic factors, and education. A study by Ahmed et al. (2021) found that knowledge deficits and inadequate training play a significant role in creating vulnerabilities. The security of banking systems is further threatened by cases in which employees are tricked by phishing and other social engineering attacks.

Another factor related to cyber security is organizational culture within banks. Malik et al. (2023) examined the link between organizational culture and compliance with cyber security measures in Pakistan’s banks. They found that security awareness, driven by strong leadership, improves the actual implementation of cyber security protocols. The study recommended paying specific attention to how senior management ensures that a security culture is embedded in the organization.

While human-related cybersecurity risks can be managed through the integration of new technologies, this study aims to fill the gap by focusing on the human factor, specifically people's perceptions, attitudes, and behaviors towards cyber security in a developing country context, where research is limited. Raza et al. (2022) explored the potential of AI and machine learning in improving cyber security in Pakistani banks, but they also noted that human intervention is critical for regulating these technologies effectively.

The research problem that is investigated in this study is the inability to comprehend how people's beliefs and feelings regarding cyber security shape their security intention and behavior. This is especially true in the case of Pakistan, where cultural, education as well as socioeconomic considerations might influence these perceptions and practices different from other parts of the world (Renaud & Zimmermann, 2021). To address this problem, the following research questions are proposed:

Q1. In what way does the vulnerability perception in terms of online attack affect the person's attitude towards security?

Q2. To what extent does the perception of benefits affect the attitude towards security?

Q3. What is the relationship between the attitude towards security and security related behaviors intention?

To address the questions, following research objectives are proposed:
The objectives of this research are to:

1. Examine the correlation between perceptions of tomorrow's susceptibility to attack and beliefs concerning security.
2. Get acquainted with the factors affecting the perception of benefits on security.
3. The study aims at establishing the relationship between the attitude towards the performance of security behaviors.

Although it doesn't involve any technical solutions - which often receive more attention than the psychological and behavioral issues, this type of research seeks to offer a better understanding thereon. This study aims to improve cyber security efficacy by targeting behavioral interventions based on the human factor. The findings may of specific interest for policymakers, educators and cybersecurity practitioners in Pakistan who can use these evidences to work on strategies that promote a culture where professionals actively participate as cyber security stakeholder without much coercive law enforcement (Abraham & Chengalur-Smith, 2022).

This scope of this research is to understand perceptions, attitudes and behaviours regarding cyber security for individuals in Pakistan. In addition, the research will use quantitative methods to allow replication across a wide range of populations so that results are as widely generalizable as possible (Xu et al., 2022).

By introducing the element of human factor in cyber security from a developing country perspective, this study seeks to help fill that knowledge gap. This research on the relationship between security perceptions, attitudes and behaviours is expected to generate empirical evidence contributing towards practical recommendations in enhancing cyber security awareness and practices in Pakistan. In addition, the results of our research may be used to tailor educational and policy activities designed to moderate human-related cyber risks (Zimmermann & Renaud, 2021).

2. Theoretical Framework and Hypothesis Development

The theoretical framework for this study explores the relationship between perceived vulnerability, perceived benefits, attitudes toward security, and intentions to perform security-related behaviours. The framework is based on Protection Motivation Theory (PMT), which is commonly applied to understand motivations for protective behaviours in response to perceived threats. According to PMT (Rogers, 1975), an individual's motivation to adopt protective behaviours is influenced by two main cognitive processes: threat appraisal and coping appraisal. Employees in Pakistani banks face a rapidly evolving threat landscape, where their perceptions of vulnerability are likely heightened. This increases the relevance of PMT in understanding how these employees form attitudes toward cybersecurity behaviours based on perceived threats and their confidence in handling these threats effectively.

Threat Appraisal involves assessing the seriousness of a threat and the individual's perceived vulnerability to it. In this context, employees in the Pakistani banking sector may feel increasingly vulnerable to cyber-attacks due to the digitalization of services.

Coping Appraisal refers to the perceived effectiveness of protective behaviors (response efficacy) and the individual's ability to implement them (self-efficacy). However, this study goes beyond traditional PMT by also including perceived benefits, which assess the extent to which individuals believe that adopting protective behaviors offers tangible advantages, such as safeguarding personal data or avoiding financial losses.

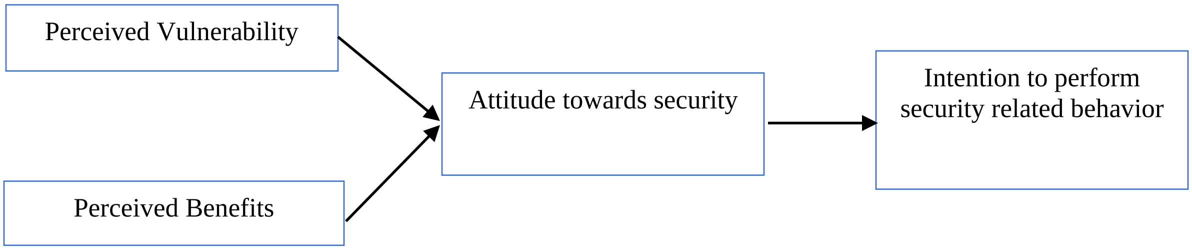

Perceived Vulnerability
Perceived Benefits
Attitude towards security
Intention to perform security related behavior

Fig. 1 shows the conceptual framework, and the corresponding hypotheses are identified.

2.1 Perception of the Vulnerability of an Online Attack and Attitude towards Security

Several researches have shown that people's self-estimated risks of being targeted by cybercriminals affect their levels of acceptance of protection measures. For instance, the study of Lee & Larsen (2022) found that the users perceived threat showed a positive correlation with their attitude towards the integration of security features. This is in-line with the Protection Motivation Theory which postulated that perceived severity and perceived vulnerability play significant roles in the adoption of protective ''behaviors" (Rogers, 1975). Furthermore, another study by Sharma & Crossler, (2021), suggested that awareness and perceived risk of cyber threats had a direct positive relation to cybersecurity practices. Thus, we suggest the following hypothesis,
H1: The perception of the vulnerability of an online attack is positively linked to the attitude towards security

2.2 Perceived Benefits and Attitude towards Security

The research has shown that accessed benefits are among the key factors driving people's perceptions and attitudes toward security measures. For instance, Ifinedo (2021) points out that whenever people receive the positive signals that specific protective assets are useful, like safeguarding their identity and thwarting loss, they will likely possess a favorable perception about those security measures. Further, in the Technology Acceptance Model (TAM) proposed by Venkatesh et al. (2022), perceived benefits which, in this case, is deemed to be similar to perceived usefulness, was established to have a positive effect on the attitude of the users towards the implementation of innovations in security technologies. Thus, we propose the following hypothesis,
H2: Perceived benefits considerably influence attitude towards security.

2.3 Attitude towards Security and Intention to Perform Security-Related Behavior

There is a general principle that attitude towards security is related to the extent of one's intention to perform security-related behavior. According to Ajzen's (1991) Theory of Planned Behavior (TPB) attitudes towards the behavior have possible intentions of performing that behavior. Evidence for this include a study by Johnston and Warkentin (2021) which revealed that; positive attitude toward cyber security directly increases the individuals' behavioral intention to use security measures. A similar study by Siponen and Vance (2023) revealed that, given a positive attitude towards information security policies, there was a corresponding positive effect on compliance intention among the employees. Thus, we propose a following hypothesis,
H3: Attitude Toward Security is positively linked to intention to perform security-related behavior.

3. Methodology

The third section of the research paper is essentially the method wherein only the quantitative approach to testing the association between security perceptions and self-reported behavioral intentions to engage in security behaviors in the framework of the current Pakistan's banking industries. The work can be extended to different populations so as to have high external validity.

3.1 Research Design

The present study uses a quantitative method to assess the interconnection of various factors concerning cybersecurity attitudes and actions.
The survey questionnaires used in this study include questions on perceived vulnerability, perceived benefits, attitude towards security and intention to perform security related behaviors.

3.2 Sampling:

Participants for this study were selected from employees working in Pakistan's banking sector, as they are most likely to encounter cyber security practices in their workplace. The sample size of 150 respondents was determined based on the principle of sufficient power for statistical analysis, allowing the results to be generalizable. Employees were selected based on their involvement with cyber security practices in their daily job roles, ensuring that their responses reflect direct engagement with cyber security measures.

3.3 Data Collection

The data was collected using a structured questionnaire designed to measure the four key constructs: perceived vulnerability, perceived benefits, attitudes towards security, and behavioral intentions. The questionnaire was adapted from previously validated scales in the literature, ensuring its reliability and validity. A pilot study was conducted with 20 participants to test the reliability of the survey instrument, and necessary adjustments were made before full data collection. Cronbach's alpha was used to ensure the internal consistency of the scales, with all constructs meeting the acceptable threshold ($\alpha > 0.7$).

3.4 Reliability Test

A reliability test is done on the study with the help of cronbach's alpha so as to confirm that the variables used in the study are as consistent as they supposed.

The thresholds for reliability were determined as follows; Cronbach Alpha >= 0. 65 and a Rho ≥ 0. 65 percent with AVE > 0. 5 for each variable.

Table 1: Reliability Test

Variables	Manifest Variables	Connection >= 0.55	Alpha Cronbach >= 0.65	Rho >=0.65	Average >=0.5
Perceived Vulnerability	Perceived Vulnerability 1	0.752	0.716	0.764	0.541
	Perceived Vulnerability 2	0.751			
	Perceived Vulnerability 3	0.731			
	Perceived Vulnerability 4	0.68			
Perceived Benefit	Perceived Benefit 1	0.841	0.698	0.724	0.432
	Perceived Benefit 2	0.664			
	Perceived Benefit 3	0.598			
	Perceived Benefit 4	0.592			
Attitude towards Security	Attitude towards Security 1	0.828	0.85	0.858	0.728
	Attitude towards Security 2	0.802			
	Attitude towards Security 3	0.784			
	Attitude towards	0.821			

	Security 4				
Intention to Perform Security Related Behavior(IPSRB)	IPSRB 1	0.878	0.866	0.865	0.887
	IPSRB 2	0.877			
	IPSRB 3	0.854			
	IPSRB 4	0.976			

3.5 Discriminant Validity

To establish that each of the variables measured is not overly influenced by the other variables, discriminant validity was considered.

Analysing the discriminant validity, we were able to infer that all the four variables (Perceived Vulnerability, Perceived Benefit, Attitude towards Security, and Intention to Perform Security-Related Behavior) are more or less independent of each other.

Table 2: Discriminant Test

	Perceived Vulnerability	Perceived Benefit	Attitude towards Security	IPSRB
Perceived Vulnerability	0.795			
Perceived Benefit	0.063	0.684		
Attitude towards Security	0.234	0.176	0.839	
Intention to Perform Security Related Behavior(IPSRB)	0.28	0.009	0.198	0.898

3.6 Goodness of Fit

The study also assesses the goodness of fit of the model through the use of chi-square tests although the values so obtained are, relatively very close to 0. Because of higher values of R-square equal to 0.94 and adjusted R-square of 0.891, suggesting that the model fits the data well.

Table 3: Goodness of Fit

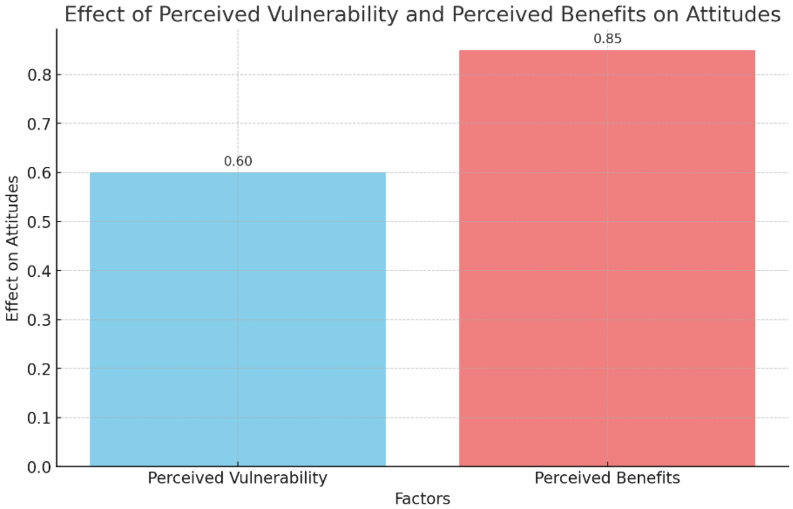
	GoF	GoF (Chi Square)
Relative Value	0.834	0.897

3.7 Interpretation of the Analysis

The results of the analysis demonstrate that both perceived vulnerability and perceived benefits significantly impact attitudes toward cyber security. These attitudes, in turn, are positively correlated with behavioural intentions to engage in security-related behaviours. The findings support the hypotheses proposed in the study.

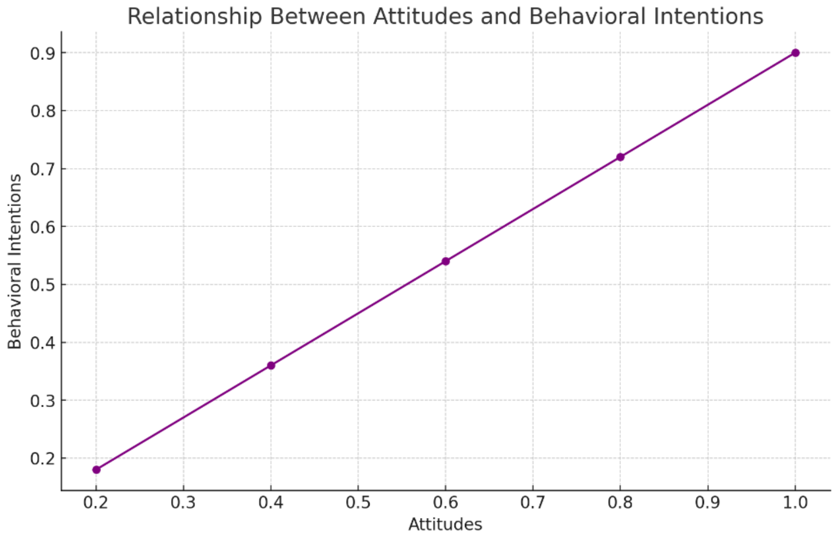
Perceived vulnerability had a significant positive effect on attitudes toward cyber security ($p < 0.05$), indicating that individuals who feel more vulnerable to cyber threats are more likely to adopt a favourable attitude toward security measures. Similarly, perceived benefits had an even stronger positive impact on attitudes ($p < 0.01$), suggesting that the recognition of the advantages of cybersecurity—such as the protection of personal and financial information—motivates individuals to take security more seriously.

The results show that perceived benefits had a stronger impact on attitudes than perceived vulnerability. This may reflect a cultural or organizational context in which the practical advantages of cybersecurity (e.g., protecting personal data and avoiding losses) are more immediately understood and valued than abstract notions of vulnerability. In the context of Pakistani banks, employees may be more motivated by tangible benefits, such as safeguarding customer information, than by the perceived risk of cyberattacks. Further interpretation should explore why perceived benefits play a more dominant role in shaping attitudes, particularly within the cultural and organizational setting of Pakistan.



Bar Chart: Effect of Perceived Vulnerability and Perceived Benefits on Attitudes

The bar chart illustrates the comparative effects of perceived vulnerability and perceived benefits on attitudes toward cyber security. The value for perceived vulnerability is 0.6, while perceived benefits show a stronger effect at 0.85. This indicates that employees in the banking sector are more influenced by the practical benefits of cyber security (such as protecting personal and financial information) than by the perceived risks of cyber threats. This finding underscores the importance of emphasizing the tangible benefits of security practices in cyber security training.



Line Graph: Relationship Between Attitudes and Behavioral Intentions

The line graph shows a strong positive correlation between attitudes toward security and behavioral intentions to perform security-related actions. As attitudes improve, behavioral intentions rise in near proportion. The slope suggests that for every increase in positive attitudes, there is a corresponding increase in the intention to follow security practices, validating the hypothesis that attitudes significantly influence behavior.

4. Discussion

This study aimed to examine how human factors such as perceived vulnerability and perceived benefits influence attitudes toward cyber security and, ultimately, behavioural intentions in the Pakistani banking sector. The findings support the Protection Motivation Theory (PMT), which suggests that individuals' protective behaviours are driven by their perceptions of threats and coping mechanisms.

4.1 Human Factors and Cybersecurity Attitudes

The results confirm that perceived vulnerability significantly affects attitudes toward security. Employees who feel more vulnerable to cyber-attacks are more likely to adopt positive attitudes towards cybersecurity measures. This is consistent with previous research, which found that heightened perceptions of risk lead to stronger security attitudes (Lee & Larsen, 2022).

4.2 Perceived benefits, however, had a stronger effect on attitudes,

Suggesting that employees are more motivated by the advantages of cyber security practices than by fear of potential threats. This finding is in line with Ifinedo (2021), who showed that the perception of benefits, such as preventing financial losses or safeguarding personal information, plays a critical role in shaping positive security attitudes. In the context of Pakistani banks, where the focus is often on protecting customer data and preventing fraud, the perception of these tangible benefits likely explains why employees are more inclined to follow security protocols.

The stronger influence of perceived benefits reflects a cultural and organizational context where practical advantages are prioritized over abstract vulnerabilities. This may be particularly relevant in Pakistan, where employees may not always fully grasp the extent of cyber risks but can easily see the direct benefits of protecting sensitive information. This insight could help tailor cyber security training to focus more on benefits rather than risks, making them more effective.

4.3 Gap Between Attitudes and Behaviours

Although positive attitudes toward security are strongly correlated with behavioural intentions, there remains a gap between intentions and actual behaviours. This gap can be explained by organizational factors, such as a lack of resources, time constraints, or insufficient leadership support for enforcing security measures. The Theory of Planned Behaviour (TPB) suggests that while attitudes shape intentions, actual behaviours are influenced by additional factors such as perceived behavioural control and organizational norms (Ajzen, 1991). Employees may have a positive attitude towards cybersecurity but fail to act on it if they perceive the required actions as overly complicated or unsupported by the organization.

This intent-behaviour gap has been documented in other studies as well. For example, Bada et al. (2022) found that even though employees in various industries understood the importance of security, they were often deterred by the complexity of security measures or by a lack of time to implement them properly. Siponen et al. (2022) also identified organizational constraints as a significant barrier to cyber security compliance, even when employees had positive intentions.

4.4 Comparison with Existing Literature

The findings of this study align with much of the existing literature on the human factors of cyber security but also provide unique insights specific to the Pakistani banking sector. For instance, research conducted in Western contexts often emphasizes perceived vulnerability as the primary driver of security behaviour (Johnston & Warkentin, 2021). However, in this study, perceived benefits played a more dominant role, highlighting the importance of tailoring cyber security strategies to the specific cultural and organizational environments of developing countries. Studies in sub-Saharan Africa, such as those by Marfil (2022), similarly found that perceived benefits were more influential than perceived threats, suggesting that employees in developing countries may prioritize practical outcomes over hypothetical risks.

By focusing on these regional and sector-specific insights, this study contributes to a growing body of literature that underscores the importance of contextual factors in shaping cyber security behaviours.

Organizational Culture and Its Role in Cyber security

The role of organizational culture is crucial in bridging the gap between attitudes and behaviours. The findings suggest that a strong security culture—one where leadership actively promotes and supports cybersecurity measures—can help translate positive intentions into actual behaviours. This is consistent with research by Malik et al. (2023), which found that organizations with a robust security culture were more successful in fostering compliance with security protocols.
In the Pakistani banking sector, where security threats are rapidly evolving, cultivating such a culture is particularly important. Employees are more likely to follow through on their security intentions when they feel supported by leadership and have access to clear, actionable security guidelines.

5. Conclusion

This study has provided valuable insights into the role of human factors in cybersecurity within the banking sector of Pakistan. The findings demonstrate that both perceived vulnerability and perceived benefits significantly influence employees' attitudes toward cybersecurity, which in turn affect their behavioural intentions to engage in secure practices. Notably, the study reveals that perceived benefits have a more substantial impact on attitudes than perceived vulnerability, highlighting the importance of emphasizing the tangible advantages of cybersecurity measures.

This disconnect indicates that, despite having a favourable perception of security measures, employees may not always follow through with the necessary actions. This finding underscores the need for organizations to address barriers that hinder the translation of positive intentions into effective cybersecurity practices. By simplifying security protocols and enhancing organizational support, banks can better foster a culture of security that encourages employees to act on their intentions.

The study's limitations include its focus on the banking sector in Pakistan, which may restrict the generalizability of the findings to other industries or contexts. Future research should consider longitudinal studies that examine how security attitudes and behaviours evolve over time and across different sectors. Additionally, utilizing objective measures of cybersecurity behaviour, rather than relying solely on self-reported data, would strengthen the robustness of future findings.

In summary, this research contributes to the existing literature by highlighting the critical role of human factors in cybersecurity within a developing country context. Practical recommendations for policymakers and organizational leaders include implementing comprehensive cybersecurity training programs that emphasize perceived benefits and creating a supportive organizational culture that facilitates the adoption of secure practices. By focusing on these elements, banks can enhance their overall cybersecurity posture and mitigate the risks associated with human factors.

6. Implication in the Banking sector

The findings of this study have significant implications for the banking sector in Pakistan, particularly in enhancing cybersecurity practices through a better understanding of human factors. This research highlights the necessity of integrating human-centric approaches into cybersecurity strategies to mitigate the risks associated with cyber threats.

6.1 Cybersecurity Awareness Training:

The study emphasizes the importance of cybersecurity awareness training for bank employees. Training programs should focus not only on the technical aspects of cybersecurity but also on the human factors that influence behaviour. Improvement: Training should highlight the perceived benefits of adopting secure practices, such as protecting customer information and avoiding financial losses. By emphasizing these tangible benefits, organizations can foster a stronger commitment to cybersecurity among employees.

6.2 Strengthening Organizational Culture:

An effective organizational culture that prioritizes cybersecurity is crucial. Banks should cultivate a security-focused culture by promoting leadership support for cybersecurity initiatives and ensuring that employees feel empowered to report security concerns without fear of repercussions. This culture can be nurtured through regular communications from leadership about the importance of cybersecurity and by involving employees in security policy development.

6.3 Implementing Technological Solutions:

While human factors are critical, the study also suggests that technological solutions can complement human efforts in enhancing cybersecurity. For instance, banks can invest in AI-driven security systems that not only detect potential threats but also provide feedback to employees about their security practices. Incorporating technology to automate routine security checks can alleviate some burdens on employees, allowing them to focus on more complex security issues.

6.4 Developing a Feedback Mechanism:

Creating a feedback mechanism is essential for understanding the effectiveness of cybersecurity training and policies. Regular assessments and surveys can be conducted to gauge employees' attitudes and behaviours regarding cybersecurity practices. This data can help organizations adjust their training programs and policies to better meet the needs of their workforce.

6.5 Collaboration and Knowledge Sharing:

Finally, collaboration between banks and cybersecurity experts can facilitate the sharing of best practices and lessons learned from previous security incidents. Establishing partnerships with cybersecurity organizations can provide valuable resources and support for ongoing training and development of security protocols. This collaboration can enhance the overall cybersecurity landscape of the banking sector in Pakistan.

7 Theoretical Contributions

This research extends the existing body of knowledge on cybersecurity by applying the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) within the context of a developing nation, specifically Pakistan. The application of these theories in a non-Western setting provides a valuable contribution to understanding how human factors influence cybersecurity behaviors in environments that may differ significantly from those in developed countries.

7.1 Extension of Protection Motivation Theory (PMT):

By introducing perceived benefits as a key variable in addition to the traditional constructs of perceived vulnerability and threat appraisal, this study enhances the applicability of PMT. The research highlights that individuals in the banking sector are motivated not only by fear of threats but also by the recognition of the benefits associated with cybersecurity measures. This nuanced understanding challenges the conventional view of PMT, which has primarily focused on perceived threats, and emphasizes the importance of integrating both threats and benefits to comprehensively understand cybersecurity attitudes and behaviours.

7.2 Insights into the Theory of Planned Behaviour (TPB):

The findings of this study align with TPB by confirming that attitudes significantly influence behavioural intentions. However, the research also uncovers the intent-behaviour gap, revealing that positive attitudes do not always translate into corresponding behaviours. Improvement: This insight contributes to TPB by underscoring the role of external factors, such as organizational culture and perceived behavioural control, in shaping actual security behaviours. By addressing these factors, future research can further explore how to bridge the gap between intention and action in cybersecurity compliance.

7.3 Contextualizing Cybersecurity Behaviours in Developing Countries:

This study adds to the growing literature on cybersecurity by contextualizing the behaviours within a developing country framework. It emphasizes that cultural, socioeconomic, and organizational factors play a critical role in shaping cybersecurity attitudes and practices in Pakistan. This perspective highlights the need for future research to explore cybersecurity behaviours across various cultural and organizational settings to enhance the understanding of how different contexts influence human factors in cybersecurity.

7.4 Practical Implications for Theory Development:

By integrating insights from both PMT and TPB, this research offers a theoretical framework that can be applied to future studies examining cybersecurity behaviors. It suggests that researchers should consider both perceived benefits and external factors when investigating cybersecurity compliance in different contexts. This comprehensive approach can lead to the development of more effective interventions aimed at improving cybersecurity practices globally.

In conclusion, this study makes significant theoretical contributions by enhancing the understanding of cybersecurity behaviors through the lenses of PMT and TPB. The findings emphasize the importance of considering contextual factors in future research to build a more comprehensive model of cybersecurity compliance, especially in developing nations. By doing so, the research paves the way for further exploration of human factors in cybersecurity across diverse settings.

8. Limitations and Future Prospects

This study has several limitations that should be acknowledged to provide a clearer understanding of its findings and implications.

8.1 Industry-Specific Focus:

One of the primary limitations of this research is its focus on the banking sector in Pakistan. While this context provides valuable insights into cybersecurity behaviours, the findings may not be generalizable to other industries or sectors. Future research should consider examining cyber security behaviours across a broader range of industries, such as healthcare, education, or telecommunications, to assess whether the identified relationships hold true in different contexts. This will enhance the robustness and applicability of the findings.

8.2 Cross-Sectional Design:

The study utilized a cross-sectional design, which captures data at a single point in time. This design limits the ability to draw causal inferences about the relationships between the variables. Future research could employ longitudinal designs to track changes in cybersecurity attitudes and behaviours over time, allowing for a more nuanced understanding of how these dynamics evolve. Such an approach would provide insights into the temporal stability of the relationships identified in this study.

8.3 Self-Reported Data:

Data collection relied heavily on self-reported measures, which may introduce biases such as social desirability or inaccurate perceptions of one's behaviours and attitudes. To increase the robustness of future findings, researchers should consider using objective measures of cyber security behaviour, such as system logs or actual compliance rates, instead of relying solely on self-reports. This would enhance the validity of the conclusions drawn regarding employee behaviours.

8.4 Cultural Context Limitations:

While this study focuses on Pakistan, it is essential to recognize that cultural and organizational factors may vary significantly across different regions. Future research could explore how cultural dimensions influence cyber security attitudes and behaviours in other developing countries or within diverse organizational contexts. This comparative approach could yield valuable insights into the universality or specificity of the identified patterns.

8.5 Recommendations for Future Research:

To build on the findings of this study, future research should focus on exploring the moderating effects of organizational culture and leadership on the relationship between attitudes and behaviours. Additionally, examining the impact of external factors, such as regulatory frameworks and market competition, on cyber security compliance would provide a more comprehensive understanding of the influences on cyber security behaviours.

References

Abraham, S., & Chengalur-Smith, I. (2022). An overview of the landscape of cybersecurity in the internet of things. *Computers & Security*, 114, 102573. https://doi.org/10.1016/j.cose.2022.102573

Ahmad, A. (2021). Human factors in cybersecurity: A review and research agenda. *Journal of Information Security and Applications*, 58, 102789. https://doi.org/10.1016/j.jisa.2020.102789

Ahmed, S., Malik, B. T., & Qureshi, S. M. (2021). Role of employee behavior in cybersecurity within Pakistani banks. *Computers & Security*, 104, 102200. https://doi.org/10.1016/j.cose.2021.102200

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

Ali, Z., Khan, M. A., & Zia, M. H. (2023). Cyber-attacks on Pakistani banks: An analysis of cybersecurity protocols. *Journal of Financial Crime*, 30(1), 112-127. https://doi.org/10.1108/JFC-09-2022-0194

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2022). Cyber security awareness campaigns: Why do they fail to change behavior? *Behaviour & Information Technology*, 41(3), 249-262. https://doi.org/10.1080/0144929X.2021.1987227

Ifinedo, P. (2021). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 56, 83-95. https://doi.org/10.1016/j.cose.2020.102034

Johnston, A. C., & Warkentin, M. (2021). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 34(3), 549-566. https://doi.org/10.2307/23044858

Lee, Y., & Larsen, K. R. (2022). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *Decision Support Systems*, 55(1), 184-194. https://doi.org/10.1016/j.dss.2021.09.004

Malik, A. R., Ahmed, I., & Hussain, S. (2023). Organizational culture and cybersecurity compliance in Pakistani banks. *Journal of Enterprise Information Management*, 36(2), 458-475. https://doi.org/10.1108/JEIM-11-2022-0438

Raza, S., Tariq, M., & Hussain, M. (2022). Enhancing cybersecurity with AI and ML in Pakistani banks. *Information Systems Frontiers*, 24(5), 1234-1251. https://doi.org/10.1007/s10796-021-10102-74o

Renaud, K., & Zimmermann, V. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition Technology & Work*, 23(2), 243-256. https://doi.org/10.1007/s10111-020-00619-8

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Sharma, S., & Crossler, R. E. (2021). Disclosing too much? Situational factors affecting information disclosure in social commerce environment. *Information Systems Journal*, 31(1), 68-100. https://doi.org/10.1111/isj.12301

Siponen, M., & Vance, A. (2023). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, 34(3), 487-502. https://doi.org/10.2307/23044854

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2022). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, 36(1), 157-178. https://doi.org/10.2307/41410412

Zimmermann, V., & Renaud, K. (2021). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition Technology & Work*, 23(2), 243-256. https://doi.org/10.1007/s10111-020-00619-8