HNSJ Humanities & Natural Sciences Journal
ISSN: (e) 2709-0833
www.hnjournal.net

Peer-Reviewed Journal
Indexed at: NSP - SJIF
Impact Factor 2022 = 4.91

RESEARCH TITLE

Exploring Factors to Improve Intentions to Adopt Cybersecurity: A Study of Saudi Banking Sector

Tariq Saeed Mian[1], Eman M. Alatawi[2]

[1] Department of IS, College of Computer Science and Engineering, Taibah University, Madinah Almunwarah, Saudi Arabia
Email: tmian@taibahu.edu.sa ORCID: 0000-0003-2666-9223
[2] Department of IS, College of Computer Science and Engineering, Taibah University, Madinah Almunwarah, Saudi Arabia. ORCID: 0000-0002-9692-3410

HNSJ, 2023, 4(9); https://doi.org/10.53796/hnsj498

Published at 01/09/2023 **Accepted at 08/08/2023**

Abstract

Ecommerce is a lynch pin of Saudi Vision 2030, which has a lot of potential but simultaneously poses risks of cyber-attacks. In the banking sector, the vision encourages financial sector growth, technological innovation, and improved access to financial services. This includes enhancing digital banking, promoting financial literacy, and enabling SME financing. Around the world the financial and banking sectors have increased their reliance on evolving technology which increased their vulnerability to face cyber-attacks. So, main objective of the study was to identify the factors that can improve cyber security among the employees of Saudi banks. Therefore, this study examined the effect of perceived usefulness, technology readiness, training and development and user satisfaction on cyber security adoption. This research also examined the mediating role of user satisfaction as well. Cross sectional research design was adopted in the present study. Data was collected from the employees of KSA private banks through survey questionnaires. Usable response rate of the study was 63.14%. The collected data was examined using Smart PLS 3.3.9. Results revealed that perceived usefulness, training and development, and technology readiness were significant predictors of user satisfaction. Similarly, user satisfaction had a significant effect on their intention to adopt cybersecurity. The mediating role of user intention was also confirmed through the results of the study. This study bridges the gap of limited studies of cybersecurity in the context of banking sector of KSA.

Key Words: *Saudi Vision 2030, Cybersecurity, User Satisfaction, perceived usefulness, technology readiness, Kingdom of Saudi Arabia (KSA), Banking*

Introduction

Ecommerce plays a pivotal role in Saudi Vision 2030 by fostering economic diversification and reducing oil dependency. It promotes digital entrepreneurship, job creation, and global trade, driving the nation's transformation into a vibrant digital economy. Concurrently, cybersecurity is paramount to safeguarding this digital ecosystem. Protecting sensitive data, ensuring secure transactions, and establishing robust defenses against cyber threats are integral to maintaining consumer trust, investor confidence, and overall sustainable growth. A resilient cybersecurity framework supports Vision 2030's goals, enabling Saudi Arabia to harness the benefits of ecommerce while mitigating risks to achieve its socio-economic objectives.

The implementation of cybersecurity, as highlighted by Li and Liu (2021), is primarily influenced by various concerns, including security and privacy. Security is also a major concern for regular computer users who utilize it at home, which consequently drives its adoption. Currently, technology collects real-time data to analyze and identify potential issues that could affect the efficient use of resources and assets. With the continuous growth of technology, cyber threats have emerged as significant risks for computer users.

One crucial aspect of technological advancement is cybersecurity, as its goal is to safeguard critical infrastructure, communication systems, and information from attacks and unauthorized access (Addae, Sun, Towey, & Radenkovic, 2019). Consequently, the significance of cybersecurity is increasing over time. Nevertheless, there is a need for further research concerning economic, social, and cultural issues and challenges to effectively adopt diverse cybersecurity practices. To ensure technology's resilience and safety, it is imperative to prioritize cybersecurity and address the mentioned challenges (Arpaci & Bahari, 2023).

Researchers have also highlighted the necessity of comprehending cybersecurity behavior and evaluating mechanisms to enhance this factor (Alhalafi & Veeraraghavan, 2023). Thus, this study aims to bridge this gap by examining the factors that can contribute to enhancing cybersecurity intentions among users."To measure the success of information system, user satisfaction is the most acceptable measure among the researchers (Sebetci, 2018). Thus, it is regarded as the critical measure to gauge the success of any system. Organizations that are considered as most successful, always prioritize customer experience as the first consideration regarding online presence, experience, and website design (Bleier, Harmeling, & Palmatier, 2019). Evaluation of users in terms of information systems is key for IT managers as it enables them to take decisions on monitoring, implementation, and adoption of the information systems. Satisfaction Vasić, Kilibarda, and Kaurin (2019) of the customers is mainly dependent on the implementation of IT related product, their reliability and security.

"Scholars Corallo, Lazoi, Lezzi, and Luperto (2022) have emphasized the need to review and assess the factors that can enhance system cybersecurity over the long term. In this context, a strong correlation exists between user behavior and perceptions of cybersecurity risks. Perceived usefulness refers to an individual's perception of how technology may improve assigned tasks. The acceptance of IT is also influenced by perceived usefulness (Mou, Shin, & Cohen, 2017). Similarly, the perceived usefulness of a system is higher when it is easily used by the user and has the potential to enhance user performance. Consequently, an increase in perceived usefulness also bolsters the intention to adopt the system (Islami, Asdar, & Baumassepe, 2021).

Technology readiness assesses and measures the maturity of technology. It's a systematic process that systematically examines the risks associated with and maturity of technology. For users, the concept of technology readiness is crucial. Marketers can determine potential adopters' profiles using this concept, which aids in communication and strategy formulation according to the adopters' profiles. Understanding the dynamics that influence technology adoption is greatly facilitated by the concept of technology readiness, as numerous researchers have explored (Berlilana, Noparumpa, Ruangkanjanases, Hariguna, & Sarmini, 2021). Scholars have reported that cybersecurity achieved through technology readiness has successfully reduced data breaches, improved security reputation, enhanced internal process security, and information processing reliability (Kaushik & Agrawal, 2021).

Minimizing internet users' uncertainty about threats requires several steps. One significant step is raising cybersecurity awareness (Catal, Ozcan, Donmez, & Kasif, 2023). This equips organizations with a knowledgeable, confident, and skilled workforce, thereby improving organizational performance by reducing user errors. Moreover, employees within the organization can better handle and identify security threats when they arise. Training helps reduce cybersecurity errors by employees. Security awareness training educates employees, as well as stakeholders like business partners and contractors (Esteves, Ramalho, & De Haro, 2017). This training helps employees comprehend how they can safeguard the organization's computer systems and data from internet-based criminals and threats. Given the evolving nature of technology and its accompanying threats, regular training is necessary (Khando, Gao, Islam, & Salman, 2021).

Hence, the primary aim of this study is to identify factors that can enhance cybersecurity intentions among banking employees in KSA. To that end, this study examines the effects of perceived usefulness, technology readiness, training and development, and user satisfaction on CAI.

Saudi Vison 2030: A Transformation

Saudi Vision 2030 is an ambitious and transformative roadmap set by the Saudi Arabian government to diversify the economy and drive sustainable development across various sectors. The pivotal roles of e-commerce and cybersecurity within this framework are critical to achieving the vision's goals of economic diversification, innovation, and global competitiveness.

E-commerce plays a central role in Saudi Vision 2030 by harnessing the power of digital technology to enhance economic growth and create new opportunities. The vision seeks to elevate Saudi Arabia as a global hub for trade and investment, with e-commerce serving as a driving force in achieving this aspiration. The Saudi Arabian General Investment Authority (SAGIA) recognizes e-commerce as a key sector to attract foreign investment and spur job creation, aligning closely with Vision 2030's objectives. The expansion of e-commerce opens avenues for entrepreneurs, small and medium-sized enterprises (SMEs), and women-owned businesses to engage in the global marketplace. This aligns with the vision's emphasis on empowering the private sector and enhancing economic diversity. (SAGIA, 2019)

However, the growth of e-commerce also introduces heightened cybersecurity challenges. As digital transactions and data exchange become more prevalent, the risk of cyber threats such as data breaches, identity theft, and financial fraud escalates. The Saudi Arabian Monetary Authority (SAMA) acknowledges the significance of cybersecurity in safeguarding digital transactions and financial stability. It emphasizes the importance of establishing robust cybersecurity frameworks to mitigate these risks and ensure consumer confidence in digital transactions. (Sama, 2021))

In response to these challenges, Saudi Arabia is actively advancing its cybersecurity capabilities to protect its digital ecosystem. The National Cybersecurity Authority (NCA) was established to oversee the country's cybersecurity strategy and collaborate with international partners to enhance cyber resilience. The NCA's initiatives include capacity-building, risk assessment, and fostering partnerships to strengthen Saudi Arabia's cybersecurity posture. (National Cybersecurity Authority (NCA), n.d.)

The synergy between e-commerce and cybersecurity is evident in Saudi Vision 2030. As e-commerce flourishes, robust cybersecurity measures are imperative to ensure the integrity of digital transactions and protect sensitive consumer information. This alignment is crucial for building a thriving digital economy where businesses can confidently engage in online transactions, consumers can shop securely, and international investors can trust in the stability of Saudi Arabia's digital infrastructure.

In conclusion, e-commerce and cybersecurity are integral components of Saudi Vision 2030's strategy to diversify the economy and drive sustainable growth. E-commerce drives economic diversification and global connectivity, while cybersecurity safeguards the digital ecosystem, fostering trust and resilience. By investing in both e-commerce expansion and robust cybersecurity measures, Saudi Arabia is poised to realize its ambitious goals and emerge as a dynamic player in the global digital economy.

Literature review

Cybersecurity

The concept of cybersecurity and cyberspace has been extensively discussed in the literature. Essentially, cyberspace refers to the interconnected web of technologies that enables the sharing of services, products, and information among participants on a broader scale. In literature, cybersecurity is defined as 'the art of ensuring the continuity and existence of an organization's information society by protecting and guaranteeing its critical infrastructure, assets, and information from criminals' (Addae et al., 2019). The primary concern of cybersecurity is to safeguard data, applications, and devices from unauthorized usage and access facilitated by internet connectivity. In the modern technological era, as most things are connected through the internet and linked to various networks, providing separate security for each computer is not feasible (Jang-Jaccard & Nepal, 2014).

Security controls are categorized into three groups: technical countermeasures, operational measures, and management measures, as defined by Addae et al. (2019). These categories are employed to ensure the protection, availability, integrity, and confidentiality of information and systems. Managerial and operational controls primarily focus on incidents and security risks that can be managed and monitored by individuals, involving training, continuity planning, business policies, and usage policies, among others. Technical controls utilize technological setups such as intrusion detection systems, encryption technologies, and user authentication as measures to safeguard systems (Abomhara & Køien, 2015). Cybersecurity threats are evolving rapidly over time due to the increasing number of users who have the capability to store, transfer, process, and gather sensitive personal and commercial information over the internet (Alromaihi, Elmedany, & Balakrishna, 2018).

Frequently, users require confirmation that their information will not be tampered with without their consent. Simultaneously, users also seek ready availability of data with convenient access whenever needed. Unfortunately, any form of data, whether personal or corporate, is at risk when accessible on the internet. Consequently, internet users should be capable of easily adopting mechanisms to minimize security risks (Sivarethinamohan, 2021). In earlier studies, Arpaci and Bahari (2023) outlined various factors related to the size of cybersecurity that may impact its adoption. These factors encompass utility, control, integration, authenticity, confidentiality, and availability.

User Satisfaction

In various studies related to technology, researchers have highlighted user satisfaction as one of the important factors for technology adoption and evaluation. Scholars have defined user satisfaction as the degree to which users believe a particular system can meet their information needs, suggesting that an information system that fulfills users' needs can bolster satisfaction. To understand user behavior in relation to the information security of a system, a key starting point is to assess user satisfaction. Considering that user satisfaction is a process rooted in contentment, if information security practices are intricate, users may encounter difficulties while utilizing the information system (Montesdioca & Maçada, 2015). In a competitive market, user satisfaction serves as a key differentiator. Additionally, analyzing user satisfaction is crucial for enhancing system performance. User loyalty to the system is also influenced by their satisfaction levels (Almarashdeh, 2016).

Perceived Usefulness

The primary objective of utilizing any system is its utility to enhance task achievement through technology. Researchers have defined usefulness as the extent to which a user assumes that a particular system can enhance performance. Based on this, Ardiansyah and Usman (2021) have defined perceived usefulness as an individual's level of belief that a certain system will improve job performance. This definition aligns with the concept of usefulness, which relates to the capacity to derive advantages.

In the context of online technologies, Saleem, Aslam, Kim, Nauman, and Khan (2022) describe perceived usefulness as the extent to which users believe that purchasing products online is beneficial. In another study, perceived usefulness is found to play a vital role in the adoption of new technology. Consequently, a user considers a technology useful if they believe that their performance will be enhanced through its use. In simpler terms, perceived usefulness significantly contributes to developing the intention among users to adopt a particular technology (Kahar, Wardi, & Patrisia, 2019).

Technology Readiness (TR)

Technology readiness involves assessing a user's readiness to adopt new technology. There are two factors within technology readiness: inhibitors and enablers. In terms of innovation, technology readiness plays a crucial role in the adoption of the latest technology. The variable of innovative technology readiness plays a critical role in influencing users' attitudes toward the use of new technology (Berlilana et al., 2021). Innovative technology readiness is a broad concept that focuses on the tendency to adopt new technology and embrace innovation (Nugroho & Fajar, 2017).

The user's mindset is evaluated through the concept of technology anxiety. This term reflects the user's willingness and ability to embrace new technologies or tools associated with emerging technology. In their previous studies, El Alfy, Gómez, and Ivanov (2017) mentioned four factors of technology readiness: insecurity, discomfort, optimism, and innovativeness.

Training & Development

Training and development play a pivotal role in enhancing the performance of an organization. Moreover, according to Mishra (2021), the adoption of new technology is significantly influenced by the training and development initiatives provided to employees. As new technologies continue to advance, the landscape of training and development has undergone transformation. Those responsible for overseeing training must recognize the evolving nature of technology and the concurrent need for improved learning processes (Santos, Trevisan, Veloso, & Treff, 2021).

The integration of new technology opens avenues for utilizing artificial intelligence across various domains. The concept of training and development embodies the notion of lifelong learning, illustrating an individual's continuous acquisition of knowledge, adaptation to change, personal growth, and value enhancement. Training and development programs hold the potential to communicate to employees that the organization's senior management is dedicated to their professional growth. This also signifies the commitment of leadership to ensuring the technological success of its workforce (Beydoun & Saleh, 2023).

With the ever-evolving technological landscape, organizations need to align their training and development strategies to address the changing skill sets required by new technologies. This can foster a culture of adaptability, innovation, and continuous improvement, ultimately leading to enhanced organizational performance and the successful assimilation of new technology.

Hypotheses development

Perceived Usefulness and User Satisfaction

Consumer behavior is influenced by a variety of factors, and researchers have identified perceived usefulness as a key predictor in the context of the online environment. User satisfaction is affected when consumers are aware of certain technologies being installed on their computers or laptops. Perceived usefulness, as indicated by Geil, Sagers, Spaulding, and Wolf (2018), refers to the extent to which an individual believes that configuring a web browser can thwart cyber-attacks.

Numerous prior studies have evaluated and confirmed the significant role of perceived usefulness in positively impacting satisfaction. Researchers define perceived usefulness as the level to which a system can substantially enhance job performance (Ramkumar, Schoenherr, Wagner, & Jenamani, 2019). Conversely, Hart, Margheri, Paci, and Sassone (2020) suggest that perceived usefulness relates to the extent to which a user believes that configuring internet security on their computer can offer protection against cyber-attacks. The adoption of any technology is positively influenced by perceived usefulness. Researchers have indicated that users are more inclined to believe that they will feel secure if proper security mechanisms are provided (Addae et al., 2019).

Technology Readiness and User Satisfaction

Past studies conducted by Hamzah, Hamzah, and Mat (2022) have highlighted the influence of technology readiness on user satisfaction. Another significant factor impacting customer satisfaction is social comfort. This suggests that users are likely to experience satisfaction if they feel at ease while using technology. Wang, So, and Sparks (2017) support this notion, indicating that user satisfaction is positively affected by their technological readiness.

Researchers such as Wiese and Humbani (2020) assert that technology readiness encompasses various constructs, serving as a variable that enhances users' acceptance of technology. The primary objective of assessing technology readiness is to gauge the maturity level of technology, thus determining its suitability for user adoption. This demonstrates the intricate relationship between user

satisfaction, social comfort, and the level of technological readiness, collectively shaping the user's perception and experience with technology.

Training & Development and User Satisfaction

Employees play a pivotal role in driving satisfaction within organizations. Particularly, the training of employees who interact with customers holds paramount importance. Employee performance receives a substantial boost when they undergo training, thereby leading to positive repercussions on customer satisfaction. Well-trained employees possess the requisite skills to effectively engage with customers. Their grasp of consumer interaction tactics and comprehension of customer needs positions them to fulfill these requirements adeptly (Shah, 2020).

Scholars Akinbowale, Klingelhöfer, and Zerihun (2020) underscore the significance of well-trained bank employees who maintain records and promptly report instances of stolen funds. Such employees effectively satisfy their clients by preventing financial losses in the event of cyberattacks. To mitigate the probability of such attacks, organizations must allocate considerable resources to training initiatives. Furthermore, customers, being end-users, require training to navigate mobile banking apps and internet-based banking to cultivate awareness about cybersecurity (Johri & Kumar, 2023).

The establishment and enforcement of procedures and policies also factor into customer satisfaction. By upholding clear guidelines, organizations are better poised to deliver consistent and satisfactory services to their customers (Kumar, Biswas, Bhatia, & Dora, 2021). In conclusion, the interconnectedness of well-trained employees, customer training, and strategic policies contributes to the overarching goal of enhancing customer satisfaction, while simultaneously fortifying the organization against potential cybersecurity threats.

User Satisfaction (US) and Intention to adopt Cyber Security

In the context of maintaining essential measures for adopting cybersecurity, user satisfaction holds a crucial role. Meanwhile, the intention to adopt cybersecurity is influenced by various factors such as education and training. When users find satisfaction in the utilization of computer-based services, it significantly impacts the adoption of online services (Kar, 2021). Similar findings were reported by Belanche, Casaló, and Guinalíu (2012), who emphasized that user satisfaction positively influenced the intention to use websites.

Based on the aforementioned discussion, the following hypotheses have been developed:

H1: Perceived usefulness (PU) has a positive effect on user satisfaction (US).

H2: Training and Development (T&D) have a significant positive effect on user satisfaction (US).

H3: Technology Readiness (TR) has a significant positive impact on user satisfaction (US).

H4: User satisfaction (US) significantly affects Cybersecurity Adaptation Intention (CAI).

H5: User satisfaction (US) mediates the relationship between Training and Development (T&D) and Cybersecurity Adaptation Intention (CAI).

H6: User satisfaction (US) mediates the relationship between Technology Readiness (TR) and Cybersecurity Adaptation Intention (CAI).

H7: User satisfaction (US) mediates the relationship between Perceived Usefulness (PU) and Cybersecurity Adaptation Intention (CAI).

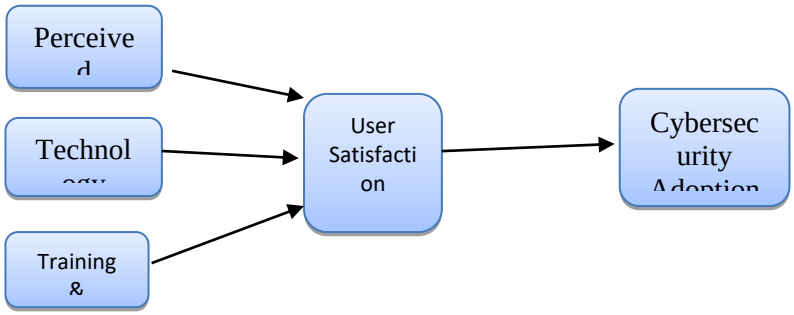


Figure 1: Research Framework

Methodology

This study employed quantitative methods based on a survey questionnaire. The research was conducted within the banks of the Kingdom of Saudi Arabia (KSA), specifically among the private banks of the KSA. Consistent with previous studies, the sample size fell within the range of 30 to 500 participants. Therefore, we distributed questionnaires to 350 employees working in private banks within the KSA. The sampling technique utilized was simple random sampling. The distribution of questionnaires was carried out personally by the researcher and the research team. In total, 296 questionnaires were collected from respondents, out of which 221 questionnaires were found usable, yielding a response rate of 63.14%. The questionnaire was divided into two sections: the first section covered demographic information about the respondents, while the second section contained information regarding the study's variables.

The questionnaire utilized in this study was adapted from previous research. The Intentions questionnaire drew from Addae et al. (2019), the user satisfaction items were derived from Boubker and Douayri (2020), perceived usefulness items were taken from Addae et al. (2019), technological readiness items were adapted from Berlilana et al. (2021), and the training and development questionnaire was adapted from Aburumman, Salleh, Omar, and Abadi (2020).

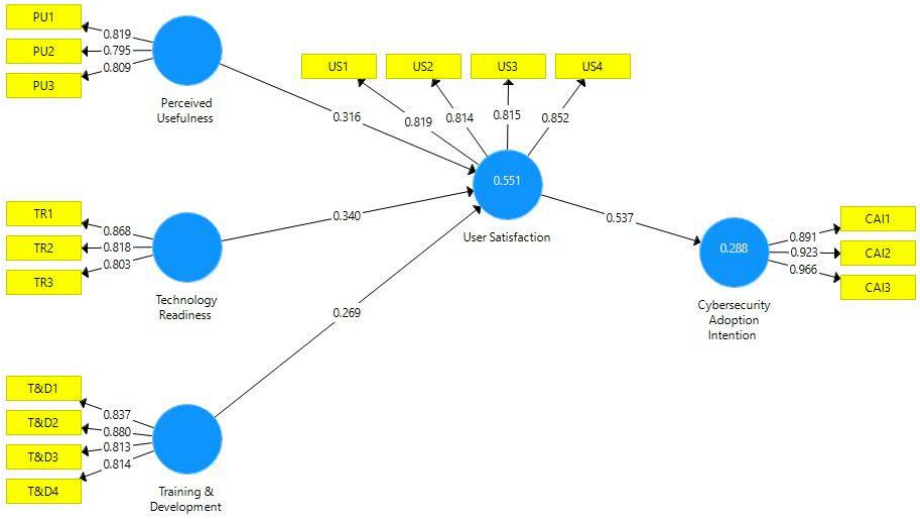
The collected data was subjected to analysis using Structural Equation Modeling (SEM), with Partial Least Squares (PLS) modeling as the chosen tool. PLS was selected due to its previous application in numerous management and social sciences studies, such as Ashraf, Ali, Khan, and Aslam (2021), and Ali, Azeem, Marri, and Khurram (2021). Furthermore, given the research's aim to predict variable dependencies, PLS-SEM was deemed the appropriate method for investigation (Ashraf, Ishfaq, Ali, & Sandhu, 2021)."

Results and Analysis

The PLS-SEM analysis comprises two stages: the measurement model and the structural model (Hair Jr, Hult, Ringle, and Sarstedt, 2021) and Ali et al., 2021). Evaluation of the measurement model involves utilizing convergent reliability, Cronbach Alpha, individual item reliability, and discriminant validity (Hair, Hult, Ringle, Sarstedt, & Thiele, 2017).

Table 1: Factor Loading

	CAI	PU	T&D	TR	US
CAI1	0.891				
CAI2	0.923				
CAI3	0.966				
PU1		0.819			
PU2		0.795			
PU3		0.809			
T&D1			0.837		
T&D2			0.880		
T&D3			0.813		
T&D4			0.814		
TR1				0.868	
TR2				0.818	
TR3				0.803	
US1					0.819
US2					0.814
US3					0.815
US4					0.852



Note: T&D= Training and Development; TR= Technology readiness; PU= Perceived Usefulness; US= User Satisfaction; CAI= Cybersecurity Adoption Intention.

Figure 1: Measurement Model

A factor loading test was conducted to evaluate the individual item reliability, as determined by Duarte and Raposo (2010). Scholars suggest that an item's reliability is established when the factor loading value exceeds 0.70. As illustrated in Table 1 and Figure 2, the factor loading for all items surpasses 0.70, confirming the achievement of individual item reliability. Subsequently, we assessed internal consistency reliability using CR and Cronbach's Alpha. According to Bagozzi and Yi (1988), the accepted threshold for CR and Cronbach's Alpha is above 0.70. As shown in Table 2, both Cronbach's Alpha and CR values substantially exceed the threshold, confirming the attainment of internal consistency.

Table 2: Reliability and Validity

	Cronbach's Alpha	**Composite Reliability**	**Average Variance Extracted (AVE)**
CAI	0.918	0.948	0.860
PU	0.734	0.849	0.652
T&D	0.857	0.903	0.700
TR	0.774	0.869	0.689
US	0.844	0.895	0.681

Note: T&D= Training and Development; TR= Technology readiness; PU= Perceived Usefulness; US= User Satisfaction; CAI= Cybersecurity Adoption Intention.

Afterward, convergent validity is evaluated using the Average Variance Extracted (AVE). The suggested AVE value should be at least 0.50 or higher (Chin, 1998). The AVE values presented in Table 2 indicate that this threshold has been met, thus confirming the achievement of convergent validity.

Table 3: Fornell and larker

	CAI	PU	T&D	TR	US
CAI	0.927				
PU	0.554	0.808			
T&D	0.748	0.570	0.837		
TR	0.413	0.324	0.528	0.830	
US	0.537	0.580	0.629	0.584	0.825

Table 4: HTMT

	CAI	PU	T&D	TR	US
CAI					
PU	**0.675**				
T&D	**0.842**	**0.722**			
TR	**0.496**	**0.435**	**0.650**		
US	**0.605**	**0.736**	**0.732**	**0.715**	

To establish discriminant validity in the current study, both the Fornell and Larcker (1981) criteria and the HTMT method were employed. For Fornell and Larcker criteria, discriminant validity is achieved when diagonal matrix values are greater than the remaining values. The values in Table 3 illustrate that all diagonal values exceed the others, confirming discriminant validity by means of Fornell and Larcker (1981) criteria.

Furthermore, the HTMT criteria were also utilized for confirming discriminant validity. As outlined by Gold, Malhotra, and Segars (2001), the construct values should not exceed 0.90. The values presented in Table 4 demonstrate adherence to this criterion, confirming the attainment of discriminant validity through HTMT criteria as well.

To address potential multicollinearity concerns, VIF (Variance Inflation Factor) was examined in the measurement model. Kock (2015) recommended a VIF value of less than 3.30. The values in Table 5 showcase that all VIF values are under 5, indicating the absence of multicollinearity issues.

Table 5: VIF

	CAI	US
PU		**1.482**
T&D		**1.838**
TR		**1.388**
US	**1.000**	

Table 6: Direct Results

		Beta	SD	T-Value	P Values	Decision
H1	**PU -> US**	0.316	0.061	5.204	**0.000**	**Supported**
H2	**T&D -> US**	0.269	0.084	3.215	**0.001**	**Supported**
H3	**TR -> US**	0.340	0.071	4.811	**0.000**	**Supported**
H4	**US -> CAI**	0.537	0.068	7.889	**0.000**	**Supported**

Following the successful validation of the measurement model, this study proceeded to test the proposed hypotheses through the structural model. Table 6 presents the outcomes of the direct hypotheses posited earlier. The results indicate that Perceived Usefulness (PU) has a significant positive impact on User Satisfaction (US), corroborating H1. Similarly, H2, which suggests a significant positive influence of Training and Development (T&D) on US, is supported by the statistical findings. Correspondingly, Technology Readiness (TR) is found to have a direct effect on US, thereby accepting H3. Furthermore, the positive association between US and Cybersecurity Adaptation Intention (CAI), as implied by H4, is upheld.

Concerning the mediating relationships, the results presented in table 7 affirm the support for H5, H6, and H7. These findings demonstrate the interconnected nature of the variables in the study and validate the proposed hypotheses.

Table 7: Indirect Results

		Beta	SD	T-Value	P Values	Decision
H5	**T&D -> US -> CAI**	0.144	0.058	2.505	**0.006**	**Supported**
H6	**TR -> US -> CAI**	0.182	0.037	4.876	**0.000**	**Supported**
H7	**PU -> US -> CAI**	0.170	0.037	4.614	**0.000**	**Supported**

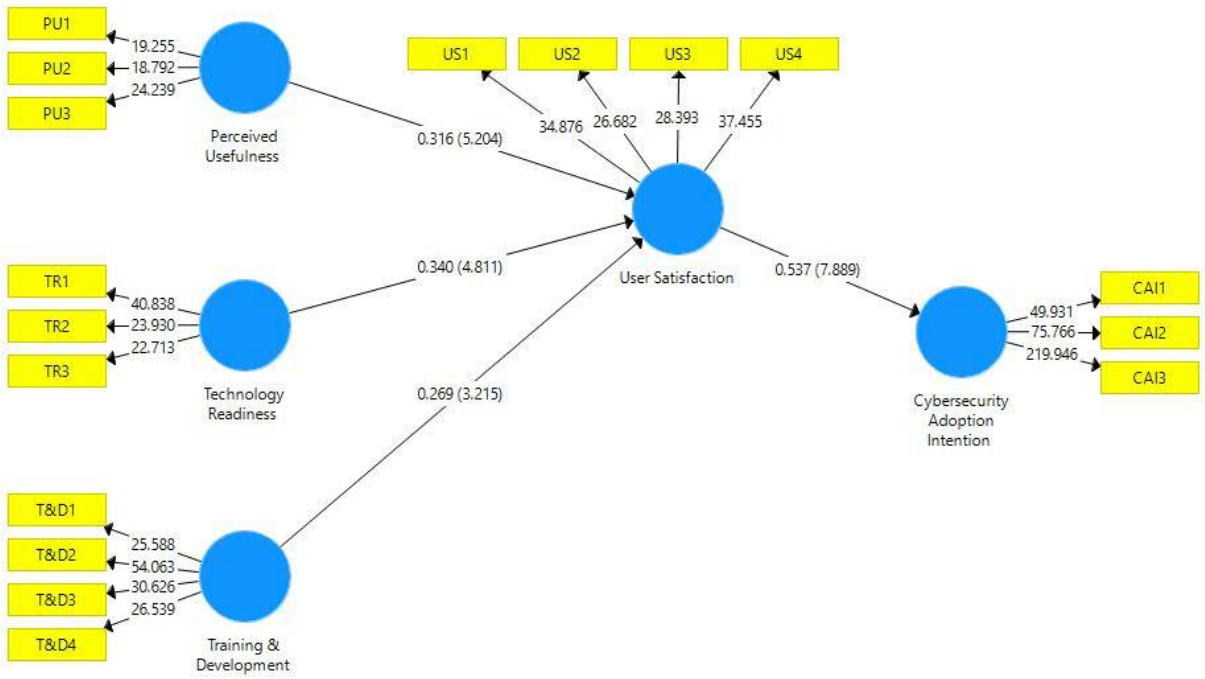
Note: T&D= Training and Development; TR= Technology readiness; PU= Perceived Usefulness; US= User Satisfaction; CAI= Cybersecurity Adoption Intention.

At the conclusion of the evaluation of the Structural model, the R square value was analyzed. The outcomes of the R square, as depicted in table 8, reveal that the mediator is influenced by 55%, while the dependent variable (DV) is affected by 28.8% through the suggested independent variables (IVs).

Table 8: R square

	R Square
CAI	0.288
US	0.551

Note: US= User Satisfaction; CAI= Cybersecurity Adoption Intention.



Note: T&D= Training and Development; TR= Technology readiness; PU= Perceived Usefulness; US= User Satisfaction; CAI= Cybersecurity Adoption Intention.

Discussion, Conclusion and Limitations

Saudi Vision 2030 constitutes a transformative roadmap formulated by the Saudi Arabian government with the aim of diversifying the nation's economy away from its traditional reliance on oil and fostering comprehensive development across multiple sectors. Specifically within the banking sector, the vision endeavors to elevate financial services, stimulate investments, and catalyze economic growth. The banking industry's strategic significance lies in its pivotal role of supporting the overarching objectives of Vision 2030. This role is manifested through the provision of vital capital for projects and enterprises, nurturing innovation in financial technology (FinTech), and extending financial services access across all societal strata. Through initiatives encompassing digital banking, FinTech innovation, and the advancement of regulatory frameworks, the banking sector attunes itself to the wider ambitions of the vision, thus contributing to the holistic diversification and sustainable advancement of Saudi Arabia's economy.

The landscape of technology is continually evolving on a global scale, and the banking sector of Saudi Arabia mirrors this dynamic trend. Yet, within this progression, employees and customers frequently encounter cyber security challenges, posing potential financial vulnerabilities. This study was conceived to evaluate the factors capable of enhancing cyber adoption intention. The study's findings shed light on the predominant role of user satisfaction as a potent predictor of Cybersecurity Adaptation Intention (CAI), in alignment with prior research by Kar (2021). Moreover, the results unveil the significant impact of perceived usefulness on user satisfaction, paralleling conclusions drawn by Hart, Margheri, Paci, and Sassone (2020) in their own research. Correspondingly, the study's outcomes underscore the pivotal influence of training and development in cultivating user satisfaction, substantiating findings akin to those of Santos, Trevisan, Veloso, and Treff (2021). Notably, the research findings accentuate the salient role of technology readiness as a key determinant of user satisfaction within the context of the Saudi banking sector, consistent with the insights posited by Wiese and Humbani (2020).

However, as with any empirical study, the present research carries certain limitations. It is anchored in a cross-sectional research design, prompting future investigations to consider adopting a longitudinal research approach while employing a similar conceptual model. Additionally, while this study's scope pertains to the Saudi banking sector, future research endeavors could extend this model to the service sector industries of other South Asian countries. The insights derived from this study could prove instrumental for decision-makers within the banking sector, enabling them to refine strategies and interventions aimed at enhancing intentions pertaining to cyber security.

References

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 65–88-65–88.

Aburumman, O., Salleh, A., Omar, K., & Abadi, M. (2020). The impact of human resource management practices and career satisfaction on employee's turnover intention. Management Science Letters, 10(3), 641-652.

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. User Modeling and User-Adapted Interaction, 29, 701-750.

Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using the balanced score card: a survey of literature. Journal of Financial Crime, 27(3), 945-958.

Alhalafi, N., & Veeraraghavan, P. (2023). Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. Smart Cities, 6(3), 1523-1544.

Ali, J., Azeem, M., Marri, M. Y. K., & Khurram, S. (2021). University Social Responsibility and Self Efficacy as Antecedents of Intention to use E-Learning: Examining Mediating Role of Student Satisfaction. Psychology and Education Journal, 58(2), 4219-4230.

Almarashdeh, I. (2016). Sharing instructors experience of learning management system: A technology perspective of user satisfaction in distance learning course. Computers in human behavior, 63, 249-255.

Alromaihi, S., Elmedany, W., & Balakrishna, C. (2018). Cyber security challenges of deploying IoT in smart cities for healthcare applications. Paper presented at the 2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW).

Ardiansyah, A., & Usman, O. (2021). The Effect of Perceptions of Usefulness, Perceptions of Ease, Perceptions of Usability on the Use of Mobile Banking. Perceptions of Ease, Perceptions of Usability on the Use of Mobile Banking (January 19, 2021).

Arpaci, I., & Bahari, M. (2023). A complementary SEM and deep ANN approach to predict the adoption of cryptocurrencies from the perspective of cybersecurity. Computers in human behavior, 143, 107678.

Ashraf, M. S., Ali, J., Khan, M. K., & Aslam, M. (2021). Examining Mediating Effect of Customer Satisfaction among Factors of Service Quality and Purchase Intention. Competitive Education Research Journal, 2(4), 105-117.

Ashraf, M. S., Ishfaq, M., Ali, J., & Sandhu, Y. A. (2021). Antecedents of Task performance and Employee Turnover: What is Mediating Role of Cognitive Trust? Competitive Education Research Journal, 2(3), 109-123.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. Journal of the Academy of Marketing Science, 16, 74-94.

Belanche, D., Casaló, L. V., & Guinalíu, M. (2012). Website usability, consumer satisfaction and the intention to use a website: The moderating effect of perceived risk. Journal of Retailing and Consumer Services, 19(1), 124-132.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761.

Beydoun, A. R., & Saleh, R. F. (2023). LITERATURE REVIEW ON TRAINING AND DEVELOPMENT IN WORK SETTING. BAU Journal-Society, Culture and Human Behavior, 4(2), 13.

Bleier, A., Harmeling, C. M., & Palmatier, R. W. (2019). Creating effective online customer experiences. Journal of marketing, 83(2), 98-119.

Boubker, O., & Douayri, K. (2020). Dataset on the relationship between consumer satisfaction, brand attitude, brand preference and purchase intentions of dairy product: The case of the Laayoune-Sakia

El Hamra region in Morocco. Data in brief, 32, 106172.

Catal, C., Ozcan, A., Donmez, E., & Kasif, A. (2023). Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Education and Information Technologies, 28(2), 1809-1831.

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. Modern methods for business research, 295(2), 295-336.

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. Computers in Industry, 137, 103614.

Duarte, P. A. O., & Raposo, M. L. B. (2010). A PLS model to study brand preference: An application to the mobile phone market. Handbook of partial least squares: Concepts, methods and applications, 449-485.

El Alfy, S., Gómez, J. M., & Ivanov, D. (2017). Exploring instructors' technology readiness, attitudes and behavioral intentions towards e-learning technologies in Egypt and United Arab Emirates. Education and Information Technologies, 22, 2605-2627.

Esteves, J., Ramalho, E., & De Haro, G. (2017). To improve cybersecurity, think like a hacker. MIT Sloan Management Review.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics: Sage Publications Sage CA: Los Angeles, CA.

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: an assessment of cyber security practices in the United States agriculture industry. International Food and Agribusiness Management Review, 21(3), 317-334.

Gold, A. H., Malhotra, A., & Segars, A. H. (2001). Knowledge management: An organizational capabilities perspective. Journal of management information systems, 18(1), 185-214.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM): Sage publications.

Hair, J. F., Hult, G. T. M., Ringle, C. M., Sarstedt, M., & Thiele, K. O. (2017). Mirror, mirror on the wall: a comparative evaluation of composite-based structural equation modeling methods. Journal of the Academy of Marketing Science, 45, 616-632.

Hamzah, A., Hamzah, M. L., & Mat, M. (2022). Measurement of Website Functionality and Perceived Usefulness in Increasing User Satisfaction through the Role of Technology Readiness for E-Learning Users. Journal of System and Management Sciences, 12(5), 252-267.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. Computers & security, 95, 101827.

Islami, M. M., Asdar, M., & Baumassepe, A. N. (2021). Analysis of perceived usefulness and perceived ease of use to the actual system usage through attitude using online guidance application. Hasanuddin Journal of Business Strategy, 3(1), 52-64.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of computer and system sciences, 80(5), 973-993.

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. Human Behavior and Emerging Technologies, 2023.

Kahar, A., Wardi, Y., & Patrisia, D. (2019). The influence of perceived of usefulness, perceived ease of use, and perceived security on repurchase intention at Tokopedia. com. Paper presented at the 2nd Padang International Conference on Education, Economics, Business and Accounting (PICEEBA-2 2018).

Kar, A. K. (2021). What affects usage satisfaction in mobile payments? Modelling user generated content to develop the "digital service usage satisfaction model". Information Systems Frontiers, 23, 1341-1361.

Kaushik, M. K., & Agrawal, D. (2021). Influence of technology readiness in adoption of e-learning. International Journal of Educational Management, 35(2), 483-495.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. Computers & security, 106, 102267.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. International Journal of e-Collaboration (ijec), 11(4), 1-10.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. Journal of Enterprise Information Management, 34(6), 1597-1629.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Mishra, R. (2021). An analysis of factors influencing omnichannel retailing adoption using ISM-DEMATEL approach: an Indian perspective. International Journal of Retail & Distribution Management, 49(4), 550-576.

Montesdioca, G. P. Z., & Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. Computers & security, 48, 267-280.

Mou, J., Shin, D.-H., & Cohen, J. (2017). Understanding trust and perceived usefulness in the consumer acceptance of an e-service: a longitudinal investigation. Behaviour & Information Technology, 36(2), 125-139.

National Cybersecurity Authority (NCA). (n.d.). About NCA. Retrieved from https://www.nca.gov.sa/en/about-nca

Nugroho, M. A., & Fajar, M. A. (2017). Effects of technology readiness towards acceptance of mandatory web-based attendance system. Procedia computer science, 124, 319-328.

Ramkumar, M., Schoenherr, T., Wagner, S. M., & Jenamani, M. (2019). Q-TAM: A quality technology acceptance model for predicting organizational buyers' continuance intentions for e-procurement services. International Journal of Production Economics, 216, 333-348.

SAGIA. (2019). Saudi Arabia's Vision 2030. Retrieved from https://www.sagia.gov.sa/en/vision2030

Saleem, A., Aslam, J., Kim, Y. B., Nauman, S., & Khan, N. T. (2022). Motives towards e-shopping adoption among Pakistani consumers: an application of the technology acceptance model and theory of reasoned action. Sustainability, 14(7), 4180.

SAMA. (2021). Cybersecurity Framework. Retrieved from https://www.sama.gov.sa/en-US/Supervision/Cybersecurity/Pages/Cybersecurity-Framework.aspx

Santos, S. A., Trevisan, L. N., Veloso, E. F. R., & Treff, M. A. (2021). Gamification in training and development processes: perception on effectiveness and results. Revista de Gestão, 28(2), 133-146.

Sebetci, Ö. (2018). Enhancing end-user satisfaction through technology compatibility: An assessment on health information system. Health Policy and Technology, 7(3), 265-274.

Shah, M. H. (2020). Employee Training on Customer Satisfaction: Mediating Role of Employee Performance and the Moderating Role of Job Autonomy. Global Journal of Human Resource Management, 8(2), 33-57.

Sivarethinamohan, R. (2021). Behavioral intentions towards adoption of information protection and cyber security (email security and online privacy): sem model. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(6), 56-68.

Vasić, N., Kilibarda, M., & Kaurin, T. (2019). The influence of online shopping determinants on customer satisfaction in the Serbian market. Journal of theoretical and applied electronic commerce research, 14(2), 70-89.

Wang, Y., So, K. K. F., & Sparks, B. A. (2017). Technology readiness and customer satisfaction with travel technologies: A cross-country investigation. Journal of Travel Research, 56(5), 563-577.

Wiese, M., & Humbani, M. (2020). Exploring technology readiness for mobile payment app users. The International Review of Retail, Distribution and Consumer Research, 30(2), 123-142.