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[1]

[1] Associate Professor, Taibah University, Madinah Almunwarah, Kingdom of Saudi Arabia

Email: TMIAN@taibahu.edu.sa

ORCID: 0000-0003-2666-9223

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 sector has 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 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 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.

Implementation of cyber security Li and Liu (2021) is mainly impacted by several different concerns like security and privacy. Security is also the main concern for the computer users who are using it at home in terms of its appropriate user which will lead to adoption of it. Presently, technology collect real time data analyze and recognize all of the issues that are possible to impact efficient use of resources and assets. As the technology is growing with the passage of time, cyber threats have become major threats for the computer users. One of the important aspect of technology development is cyber security because its objective is to protect critical infrastructure communication systems, and information from attacks and unauthorized access (Addae, Sun, Towey, & Radenkovic, 2019). Therefore, the importance of cybersecurity is mounting with the passage of time. Despite that, there is need of more research in terms of economic, social and cultural issues and challenges in order to adopt different practices of cybersecurity. In order to ensure technology resilience and safety, it is key to prioritize cybersecurity as well as to address the mentioned challenges (Arpaci & Bahari, 2023). Researchers have also mentioned that there is need to understand the behavior of cybersecurity and assess the mechanism to enhance that behaviour (Alhalafi & Veeraraghavan, 2023). Thus, this study intends to fill this gap by examining the factors that can help in improving cybersecurity intentions among users.

To measure the success of information system, user satisfaction is 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 forward-looking and successful looking always consider 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 the key for the 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 pointed that there is need to review and assess the factors that can improve the cybersecurity of the system and improve it on the long term basis. In these terms, there is strong correlation among behavior of user and perception regarding cybersecurity risks. Perceived usefulness is regarded as perception of the individual the regarding the technology may improve the tasks assigned. Acceptance of IT is also influenced by the perceived usefulness (Mou, Shin, & Cohen, 2017). On the other hand, perceived usefulness of the system will also be high if any system is easy to use by the user and has tendency to improve the performance of user as well. Thus, if the perceived usefulness of the user increase, it will also enhance the intention to adopt the system as well (Islami, Asdar, & Baumassepe, 2021).

Technology readiness is the way to assess and measure the maturity of the technology. Assessment of technology readiness is the metric based, systematic process that has tendency to examine the risks associated with and maturity of the technology. For the users, the construct of technology readiness is very important. The profile of potential adopters can be determined by the marketers with the help of this construct that will later help in communicating and formulating the strategies according to adopter’s profile. The construct of technology readiness is very important in order to understand the dynamics that can influence adoption of technologies. A number of different researchers have examined the impact of this construct (Berlilana, Noparumpa, Ruangkanjanases, Hariguna, &

Sarmini, 2021). Scholars have reported that cybersecurity achieved through technology readiness have successfully reduced breaches of data, improved reputation of security, improved security of internal processes and reliability of the information processing (Kaushik & Agrawal, 2021).

There is a need to take a number of different steps to minimize the uncertainty of threats that are faced by the users of internet. One of the key steps is the awareness of the cybersecurity (Catal, Ozcan, Donmez, & Kasif, 2023). It provides the organizations the workforce that is knowledgeable, confident and skilled. As a result, the performance of the organization is also bound to improve as the chances of error by the users are reduced. Furthermore, employees working in the organization can better handle and identify security threats in situations when they arise. The cybersecurity mistakes by the employees can be reduced by their training. The security awareness training the process in order to educate the employees and other stakeholders like business partners and contractors (Esteves, Ramalho, & De Haro, 2017). This training helps the employees to understand the way they can protect the computer systems and data of the organization from criminals and threats that can be done through internet. There is need of training on the regular basis as technology is being evolved on the regular basis increasing the level of threat as well (Khando, Gao, Islam, & Salman, 2021). So, the main purpose of this study is to identify the factors that can improve cyber security intentions among banking employees of KSA. In this regard, this study examined effect of perceived usefulness, technology readiness, training and development, and user satisfaction on CAI.

Saudi Vison 2030: A Transformation

E-commerce and cybersecurity play integral roles in Saudi Vision 2030, a comprehensive roadmap launched by the Saudi Arabian government to diversify the economy, reduce its dependency on oil, and drive sustainable development. This ambitious vision encompasses various sectors, and the integration of e-commerce and robust cybersecurity measures is essential to its success.

E-commerce, defined as the buying and selling of goods and services over the internet, is a cornerstone of Saudi Vision 2030. The vision seeks to transform Saudi Arabia into a global investment powerhouse and a hub connecting three continents. E-commerce serves as a catalyst for achieving this goal by fostering entrepreneurship, attracting foreign direct investment, and expanding the reach of Saudi businesses beyond traditional boundaries. It promotes the growth of small and medium-sized enterprises (SMEs) and empowers youth and women to participate in the economy through digital platforms. By facilitating access to a global marketplace, e-commerce contributes to economic diversification and job creation.

However, as e-commerce flourishes, the importance of cybersecurity becomes even more pronounced. The increased digital connectivity brings about heightened risks of cyberattacks, data breaches, and financial fraud. Safeguarding the digital infrastructure and the personal information of citizens, businesses, and institutions is a paramount concern. Saudi Arabia's Vision 2030 recognizes the critical role of cybersecurity in maintaining trust, fostering innovation, and ensuring the continuity of digital services.

To realize the vision's objectives, the Saudi government is actively investing in cybersecurity initiatives. This includes the establishment of regulatory frameworks and standards for data protection, privacy, and online transactions. Collaborations with international cybersecurity organizations and experts facilitate knowledge sharing and capacity building. Additionally, initiatives to enhance cybersecurity education and awareness help build a skilled workforce equipped to combat emerging cyber threats.

The synergy between e-commerce and cybersecurity in Saudi Vision 2030 is evident through various strategies. The growth of e-commerce relies on secure digital transactions and protected customer data. Robust cybersecurity measures, such as encryption, firewalls, and multi-factor authentication, instill confidence in consumers, encouraging them to embrace online shopping and electronic payments. Furthermore, e-commerce platforms must comply with stringent cybersecurity regulations to prevent cybercriminals from exploiting vulnerabilities.

As mentioned before, Saudi Vision 2030 is a strategic plan by the Saudi Arabian government to diversify the economy and reduce reliance on oil and aims to transform the country into a global investment hub and foster social and economic development. 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. The sector's evolution aligns with the broader goals of economic diversification, job creation, and sustainable growth outlined in Saudi Vision 2030.

In conclusion, e-commerce and cybersecurity are two interconnected pillars of Saudi Vision 2030 that contribute to economic transformation, diversification, and resilience. E-commerce drives economic growth by opening up new avenues for trade and entrepreneurship, while cybersecurity ensures the safety and integrity of digital transactions and infrastructure. Together, these elements empower Saudi Arabia to become a leading player in the global digital economy while safeguarding its citizens and businesses from evolving cyber threats. By fostering innovation, enabling secure digital interactions, and nurturing a culture of digital trust, e-commerce and cybersecurity propel Saudi Arabia towards the realization of its visionary goals by 2030.

Literature review

Cybersecurity

Literature has discussed the concept of cybersecurity and cyberspace on a number of places. Basically, cyberspace is the interconnection of web technology that enables the sharing of services, products, and information available to the participants on the broader range. In literature, cybersecurity is defined as “the art of continuity and existence of information society of an organization protecting and guaranteeing its critical infrastructure, assets and information from criminals” (Addae et al., 2019). The main concern of cybersecurity is to protect the data, applications and devices from the unauthorised usage and access that is possible through internet connectivity. In modern technology and era, most of the things are being connected through internet and attached to different networks, it is not possible to provide separate security on each computer (Jang-Jaccard & Nepal, 2014).

The security controls are classified into three categories namely technical countermeasures, operational measures and management measures by the Addae et al. (2019). These categories are applied for the protection, availability, integrity and confidentiality of the information and system. The focus of managerial and operational controls is on the incidents and security risks that can be managed and monitored by people for training, continuity planning, business and usage policies etc. technical control is the mechanism that use set-ups on the basis of technology such as intrusion detection systems, encryption technologies and user authentication as measures to protect the systems (Abomhara & Køien, 2015). The cybersecurity threats are being evolved rapidly with the passage of time as more and more users have the ability to store, transfer, process and gather sensitive personal and commercial information over the internet (Alromaihi, Elmedany, & Balakrishna, 2018).

Most of the times, users need confirmation that information without their consent will not be tempered. On the other hand, users also want the readily availability of the data along with its access whenever they want. Unfortunately, any kind of data, personal or corporate is at risk that is accessible on the internet. Consequently, the users of internet should be able to easily adopt any mechanism to minimize the risk of security (Sivarethinamohan, 2021). In past studies Arpaci and Bahari (2023), size factors of cybersecurity are mentioned that may impact its adoption. These factors include utility, control, integration, authenticity, confidentiality and availability.

User Satisfaction

In different studies related to technology, researchers have mentioned that user satisfaction is one of the important factor for the adoption and evaluation of technology. Scholars have defined, satisfaction of user as the level to which it is believed by the user that certain system has the ability to satisfy their information needs, proposing that information system that fulfils the needs of the users can reinforce the satisfaction. In order to diagnose the user’s behavior in relationship with information security of the system, the key starting point is to assess the satisfaction of the users. Keeping in view that user satisfaction is the process that is based on satisfaction, if the practices of information security are complex, difficulties will be encountered by the users while using information system (Montesdioca & Maçada, 2015). In competitive market, key differentiator is the user satisfaction. Additionally, in order to improve the performance of system, it is very important to analyze the satisfaction of user. Loyalty of the user for the system is also impacted by the user satisfaction (Almarashdeh, 2016).

Perceived Usefulness

The main objective of using any system is to be useful so it can improve achievement of the task by the technology. Researchers have defined usefulness as to how far it is assumed by the user that certain system has the ability to improve the performance. On these grounds, Ardiansyah and Usman (2021) has defined perceived usefulness as the level of individual's belief that job performance will be improved by using certain system. This definition is aligned with the definition of usefulness which is the ability to use the advantage. In terms of online technologies Saleem, Aslam, Kim, Nauman, and Khan (2022), perceived usefulness is described as the extent to which it is it is believed by the users that purchasing products online is useful. In another study, in order to adopt new technology, perceived usefulness plays very important role. Therefore, user perceives a technology useful if it is believed by the user that performance will be upgraded by the use of any certain technology. In other words, PU plays integral role to develop intention among user to adopt any technology (Kahar, Wardi, & Patrisia, 2019).

Technology Readiness (TR)

Technology readiness involves measurement of user's readiness to use any technology that is new. There are two factors to technology readiness namely inhibitors and enablers. Technology readiness in terms of innovation plays very important role for the usage of latest technology. The variable of innovative technology readiness plays critical roles in altering attitude of users towards usage of any new technology (Berlilana et al., 2021). Innovative technology readiness is a very broad terminology that has focus on the tendency to adopt new technology and innovativeness (Nugroho & Fajar, 2017). The state of mind of the user is assessed through technology anxiety. This term express the willingness and ability of the user to adopt new technologies or tools related to any new technology. Researchers in their past El Alfy, Gómez, and Ivanov (2017) studies have mentioned four factors of TR namely insecurity, discomfort, optimism and innovativeness.

Training & Development

Training and development within a firm is the important factor to improve its performance. On the other hand, Mishra (2021) adoption of new technology is also influenced by the training and development of the employees. With the advancement of new technology, the implementation of training and development is totally changed. It is very important for the personal dealing with training and development that technology is being evolved on the regular basis and learning process is also being improved as well (Santos, Trevisan, Veloso, & Treff, 2021). With the advancement of new technology, it is possible to use artificial intelligence for a number of different matters. The term training and development means the lifelong learning. It explains the way an individual learn something on regular basis, accommodate with change, grow & improve, adjust, fit to changes, and add value. The programs related to training and development convinces the employees that the top management of the organization care about professional development of the employees. Moreover, the top management is committed in success of the employees in terms of technology (Beydoun & Saleh, 2023).

Hypotheses development

Perceived Usefulness and User Satisfaction

Consumer behavior is impacted by several different factors. Among these, researchers have mentioned perceived usefulness as one of the key predictor in the context of online environment. The satisfaction of the user is influenced if consumers understand that certain technology is installed in their computers or laptops. Perceived usefulness Geil, Sagers, Spaulding, and Wolf (2018) refers to the level to which an individual believes that setting of web browser can prevent any cyber-attack.

A number of past studies have assessed and confirmed the significant role of perceived usefulness in positively impacting satisfaction. Researchers have defined PU as the level to which a system can play an integral role to improve its job performance (Ramkumar, Schoenherr, Wagner, & Jenamani, 2019). On the other hand, Hart, Margheri, Paci, and Sassone (2020) perceived usefulness refers the level to which a user believed setting of the internet security is the computer can provide protection against cyber-attacks. Adoption of any technology is positively impacted by the perceived usefulness. It is mentioned by the researchers that it is more likely that if users believe that users will feel secured if proper security mechanism is provided to them (Addae et al., 2019).

Technology Readiness and User Satisfaction

Several past studies Hamzah, Hamzah, and Mat (2022) have reported that satisfaction of the user is impacted by the technology readiness. Also, social comfort is an integral determinant that influences the satisfaction of the customers. In these lines, it is assumed that if customers use technology, they will feel satisfied if they get relaxed as result of it. Based on it Wang, So, and Sparks (2017), it is inferred that satisfaction will be positively influenced by the technological readiness of the user.

According to researchers, Wiese and Humbani (2020) technology readiness is the variable of several different constructs. It includes factors that improve the technology acceptance by the users. The main objective of technology readiness is to examine the level the maturity of the technology so they can be adopted by the users.

Training & Development and User Satisfaction

Employees are an integral part of achieving satisfaction. Training of the employees who are dealing with customers is very important. The performance of the employees will be very good if they are trained. Thus, the satisfaction of the customers will be positively impacted as well. The well-trained employee has the skill to deal with the customers. They have understanding regarding tactics to deal with consumers, and they also have understanding regarding needs of the customers. Therefore, they play very important role to satisfy the customers by fulfilling these customers' needs (Shah, 2020). According to scholars Akinbowale, Klingelhöfer, and Zerihun (2020), the employees of banks who are well trained and keep record and prompt reporting of the stolen funds, are successfully able to satisfy their clients because the clients never face the issue of financial loss in case of cyberattacks.

In order minimize the probability of such attacks; organizations need to spend a lot of capital on the training. On the other hand, customers (as they are users) also need training to use mobile banking apps and banking by using internet to get awareness of cybersecurity (Johri & Kumar, 2023). Also, if organizations can maintain procedure and policies, they will be able to keep their customers satisfied (Kumar, Biswas, Bhatia, & Dora, 2021).

User Satisfaction (US) and Intention to adopt Cyber Security

In order to maintain the measures that are important to adopt cyber security, user satisfaction plays very important role. Whereas intention to adopt cybersecurity is impacted by a number of different factors like education, training etc. If the user is satisfied with the usage of any computer based service, it will have significant impact on the adoption of that online service (Kar, 2021). Same findings were reported by Belanche, Casaló, and Guinalíu (2012) who pointed that intention to use website was positive influenced by user satisfaction.

Following hypothesis are developed in the basis of above discussion.

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

H2: Training and Development (T&D) has significant positive effect on US.

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

H4: US has significant effect on CAI (Cybersecurity Adaptation Intention).

H5: US mediates the relationship between T&D and CAI.

H6: US mediates the relationship between TR and CAI.

H7: US mediates the relationship between PU and CAI.

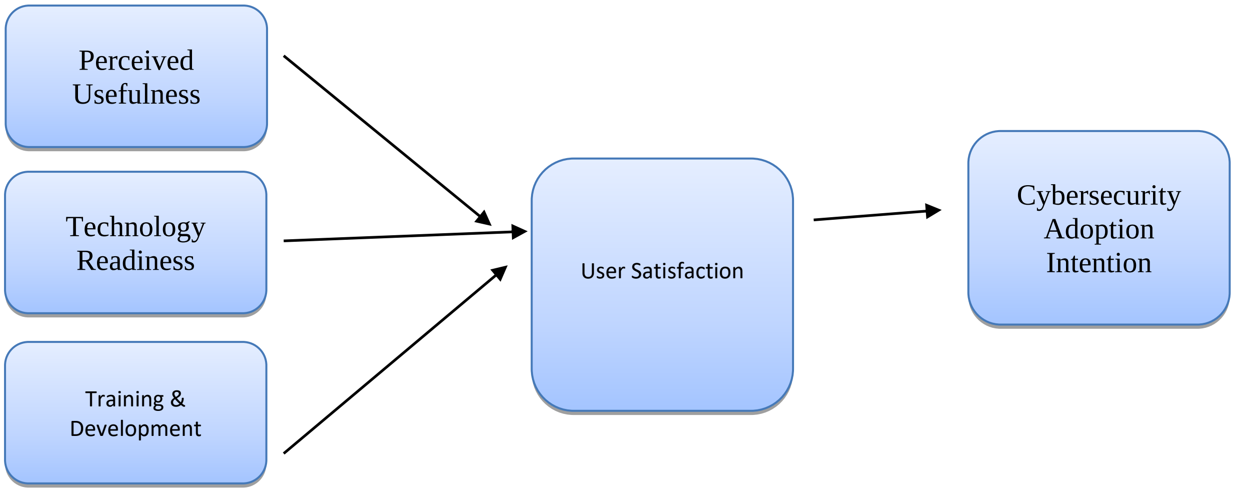


Figure 1: Research Framework

Methodology

In this study, we used quantitative methods on the basis of survey questionnaire. This study was conducted in the banks of Kingdom of Saudi Arabia. For this study, the sample was collected from the private banks of the KSA. According to past studies, the threshold level of sample is between 30 to 500. Therefore, we distributed questionnaire among 350 employees who are working in private banks of KSA. The sampling technique used in this research is simple random sampling. The questionnaire was distributed personally by the researcher and team. We received back 296 questionnaires from the respondents. Among these, 221 questionnaires were usable having the response rate of 63.14%. The questionnaire was distributed in two sections i.e. demographical information regarding respondents (in 1st section) and information regarding variables of the study in second section.

The questionnaire of the study was adapted from the past studies. The questionnaire of Intentions was adapted from Addae et al. (2019), items of user satisfaction were adapted from Boubker and Douayri (2020), items of perceived usefulness were adapted from Addae et al. (2019), items of technological readiness is adopted from Berlilana et al. (2021), and questionnaires of training and development were adapted from Aburumman, Salleh, Omar, and Abadi (2020). The collected data was later assessed using SEM as technique and PLS modelling as tool for the analysis of the collected data. In this study, PLS was used as it is previously used in a number of studies related to management and social sciences Ashraf, Ali, Khan, and Aslam (2021) and Ali, Azeem, Marri, and Khurram (2021). Moreover, aim of this research was to predict the dependence of the variable therefore, PLS-SEM was considered more suitable as method to investigate (Ashraf, Ishfaq, Ali, & Sandhu, 2021).

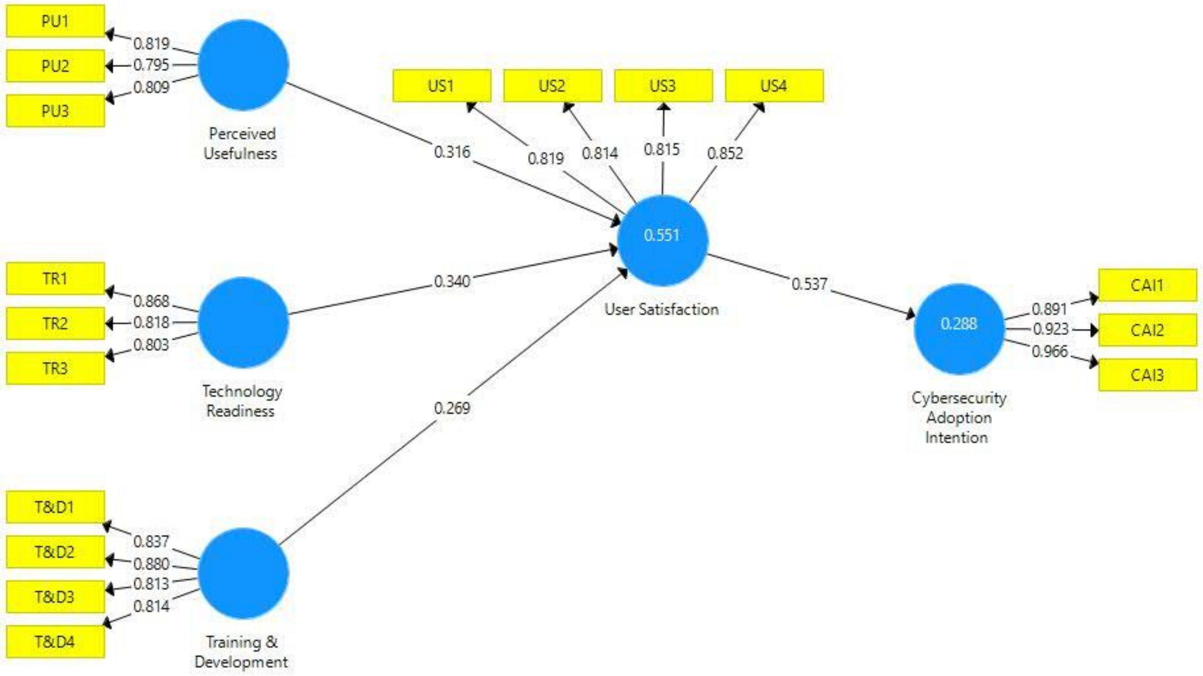
Results and Analysis

Researchers suggested that analysis through PLS-SEM is based on two stages i.e. measurement model and structural model Hair Jr, Hult, Ringle, and Sarstedt (2021) and Ali et al. (2021). The assessment of measurement model was based in the utilization of 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.



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

Figure 1: Measurement Model

Factor loading test was conducted for the assessment of individual items reliability as determined by Duarte and Raposo (2010). Scholars suggested that the reliability of the items is determined if the value of factor loading is more than 0.70. It is evident from Table 1 and figure 2 that factor loading of all items is above 0.70. Thus, individual item reliability is achieved. Later, we assessed internal consistency reliability through CR and Cronbach Alpha. According to Bagozzi and Yi (1988), the threshold level of CR and Cronbach Alpha is more than 0.70.In table 2, it is evident that Cronbach Aloha and CR values are well above the threshold level. Thus, internal consistency is achieved.

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.

Later, convergent validity is assessed through AVE. The recommended value of AVE should be minimum 0.50 or more (Chin, 1998). The values of AVE in table 2 show that this threshold level is achieved, confirming 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

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

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**	

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

In order to determine discriminant validity in the present study, Fornell and Larcker (1981) criteria and HTMT method was used. Discriminant validity by using Fornell and Larker criteria is achieved if all values of matrix placed at diagonal are more than the remaining values. The values in table 3 shows that all values at diagonal are more than other values of matrix. Thus, discriminant validity through Fornell and Larcker (1981) criteria. Moreover, we also used HTMT criteria for the discriminant validity confirmation. According to Gold, Malhotra, and Segars (2001) the construct’s values must not go beyond 0.90. The values in table 4 show that this criteria is fulfilled. Thus, discriminant validity is achieved through HTMT criteria as well. In the end of measurement model, we also examined VIF to confirm the issue of multicollinearity Kock (2015) proposed the value of VIF to be less than 3.30 and table 5 shows all values of VIF is less than 5 confirming no issue of multicollinearity.

Table 5: VIF

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

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

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**

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

After successful assessment of measurement model, this study evaluated the proposed hypothesis through structural model testing. Table 6 represents the results of direct hypothesis proposed earlier. Results shows that PU has significant positive impact on US, accepting H1. Similarly, H2 of the study is accepted as statistical findings shows that T&D has significant positive impact on US. Likewise, TR has direct effect on US, accepting H3. In the end, US also have positive relationship with CAI, supporting H4. In terms of mediating relationships, findings given in table 7 shows that H5, H6 and H7 are supported as well.

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**

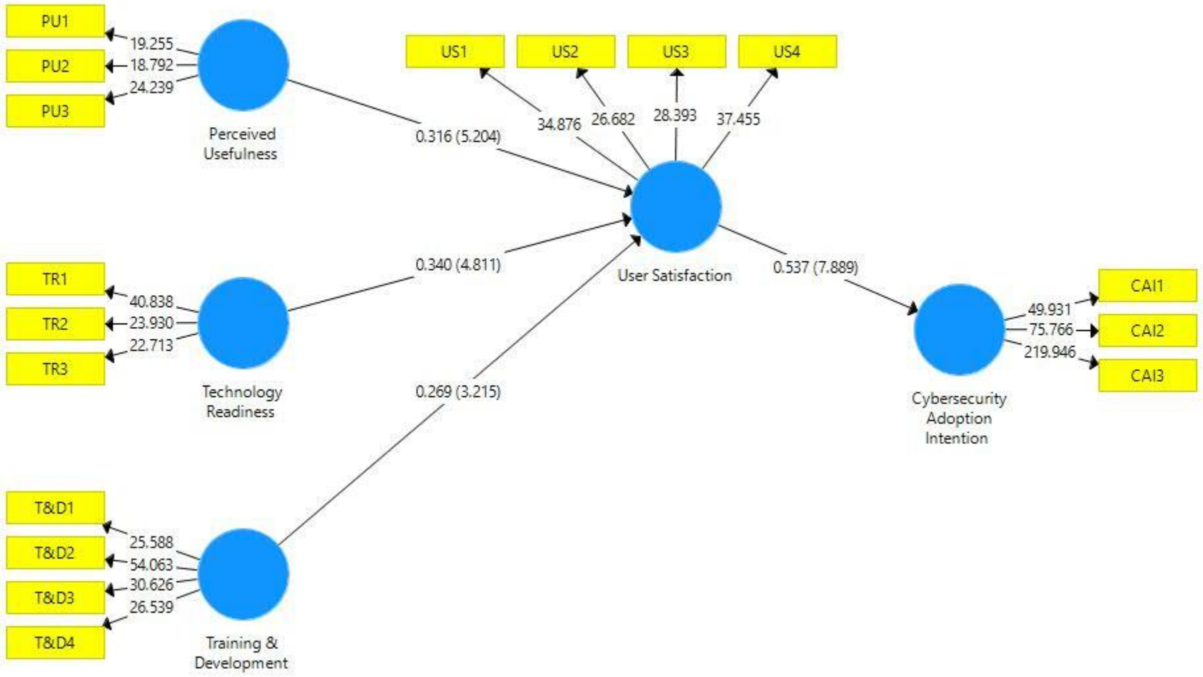
Note: T&D= Training and Development; TR= Technology readiness; PU= Perceived Usefulness; US= User Satisfaction; CAI= Cybersecurity Adoption Intention.

In the end of Structural model assessment, R square value was examined. Results of R square in table 8 shows that mediator is impacted 55% and DV is impacted 28.8% through the proposed IV’s.

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 is a transformative roadmap laid out by the Saudi Arabian government to diversify its economy beyond oil dependency and stimulate comprehensive development across various sectors. In the context of the banking sector, this vision aims to enhance financial services, boost investment, and encourage economic growth. The banking sector's role is pivotal in supporting Vision 2030's goals by providing the necessary capital for projects and businesses, fostering innovation in financial technology (FinTech), and expanding access to financial services for all segments of society. Through initiatives such as digital banking, FinTech innovation, and improved regulatory frameworks, the banking sector aligns itself with the vision's broader objectives, contributing to the overall economic diversification and sustainable growth of Saudi Arabia.

Technology is being evolved around the globe. Same is the situation in the banking sector of KSA. Employees and customers often face cyber security Issues which can create financial loss. Therefore, this study was designed to assess the factors that can improve cyber adoption intention. Findings of the study reveals that user satisfaction is the major predictor of CAI. These findings are inline with the results of (Kar, 2021). Additionally, findings demonstrate that perceived usefulness significantly effects the user satisfaction. In past, Hart, Margheri, Paci, and Sassone (2020), revealed same results in their research as well. Likewise, results reflects that training and development plays important role to develop satisfaction among the user. It is because the person who is trained person can take certain steps to avoid cyber threat. In past, Santos, Trevisan, Veloso, and Treff, (2021) presented same results. In the end, according to findings, technology readiness is also important factors of user satisfaction in the context Saudi banking sector Wiese and Humbani (2020).

There are few limitations in the present study similar to other empirical studies. This study used cross sectional research design. Future studies can use longitudinal research design while applying similar conceptual model. Moreover, this study is conducted in the context of KSA banking sector. Whereas future studies can apply this model in the context of any other service sector industry of South Asian countries. The results of the present can be used by the decision makers of the banking sectors to improve intentions regarding 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, 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.

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.

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.

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.

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.

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.