smart cities

MDPI

Hypothesis

Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model

Nawaf Alhalafi * and Prakash Veeraraghavan

Department of Computer Science and Information Technology, La Trobe University, Bundoora, VIC 3086, Australia; p.veera@latrobe.edu.au
* Correspondence: 17814379@students.latrobe.edu.au

Abstract: This study aims to explore the challenges and issues in adopting cybersecurity practices in smart Saudi cities and to develop and validate a newly developed cybersecurity-based unified theory of acceptance and use of technology 3 (UTAUT3) model. The study has a twofold purpose. First, it identified the key challenges and issues in adopting smart cities in Saudi smart cities. Second, it developed a technology-based model to adopt cybersecurity practices in Saudi smart cities. Two surveys were conducted to achieve these objectives. The first survey identified challenges and gaps in adopting cybersecurity practices in smart cities, revealing concerns about weak cybersecurity platforms, privacy breaches, and the impact of IT infrastructure advancements on Saudi culture (N = 554: common public). The second survey focused on developing and validating a cybersecurity-based UTAUT3 model (N = 108: IT professionals), emphasizing nine factors: performance expectancy, effort expectancy, social influence, facilitating conditions, safety, resiliency, availability, confidentiality, and integrity of cybersecurity. The model's validity and reliability were assessed, demonstrating its potential for understanding user behavior and adoption patterns in smart cities. The study findings provide valuable insights into the factors influencing the adoption of cybersecurity measures in smart Saudi cities, highlighting the need for targeted strategies, effective awareness programs, and collaboration between stakeholders to promote a secure and resilient digital environment. Future research may focus on refining the model, extending its applicability to other regions or countries, and investigating the impact of emerging technologies and evolving cyber threats on user behavior and cybersecurity practices.

Keywords: cybersecurity-based UTAUT3 model; conceptual development; validation; smart Saudi cities

Citation: Alhalafi, N.; Veeraraghavan, P. Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities: Conceptualization of the Cybersecurity-Based UTAUT Model. *Smart Cities* **2023**, *6*, 1523–1544. https://doi.org/10.3390/smartcities6030072

Academic Editors: Luis Hernández-Callejo, Sergio Nesmachnow and Pedro Moreno-Bernal

Received: 1 May 2023
Revised: 19 May 2023
Accepted: 24 May 2023
Published: 29 May 2023

1. Introduction

Smart cities are emerging as an innovative solution to the challenges urban areas face in the 21st century. They integrate digital technology, data, and connectivity to improve the quality of life for citizens and foster sustainable development [1]. In recent years, various countries have strongly committed to implementing smart city initiatives, with ambitious projects to create intelligent urban environments [2]. Developing smart cities is becoming a top priority as these countries strive to diversify their economies and reduce dependency on traditional industries. However, implementing these innovative urban environments raises critical concerns related to cybersecurity, given the increased connectivity and reliance on digital infrastructure [3]. As the potential for future possibilities attracts people from various parts of the country and the world, the rapid population growth in these smart cities has highlighted significant security concerns and increased the informal economy [4]. Ensuring the safety and security of citizens, infrastructure, and data in smart cities remains a pressing issue that needs to be addressed to fully realize the potential benefits of these innovative urban environments.

Similarly, the smart cities in Saudi Arabia faced the same challenges. They reflected a 689% rise in residents compared to a 146% rise globally over the previous 56 years [5]. Identification of criminal activities, technological innovation, an excellent educational system, modern hospitals, and other social services are all required because of Saudi Arabia's growing population [6]. Smart facilities, networks, smart waste management framework, and smart management systems are all required because of Saudi Arabia's growing population. Technology today, such as cybersecurity systems, supports real-time data collection, recognizes, and analyzes possible issues to efficiently accomplish assets and resources [6]. In addition, Mohammad and Abdulqader [7] conducted a study of finding cybersecurity requirements in Saudi smart cities. They concluded that significant concerns include privacy, data security, and preventative measures. The proposed solutions in the research may be sufficient on their own, but it needs to be clarified what would occur if all of these solutions were combined into a single comprehensive system.

Smart cities worldwide, including those in development, still need to universally establish comprehensive action plans that detail their strategies to respond to potential cyberattacks targeting their facilities, infrastructure, and information and communication technology systems. Weaknesses in any one component can have far-reaching implications due to the inherent interconnectedness of all processes. As a result, recommendations should be made available to the organizations responsible for selecting and vetting the technologies that will be utilized in smart cities globally. As smart cities continue to grow and integrate advanced digital technologies, they become increasingly susceptible to cyber threats [8]. Cybersecurity is a crucial aspect of smart city development, as it aims to protect information, communication systems, and critical infrastructure from unauthorized access and attacks [9]. Despite the growing importance of cybersecurity, more research is needed on the cultural, social, and economic challenges and issues in adopting cybersecurity practices in smart cities worldwide [10]. Addressing these challenges and prioritizing cybersecurity will be essential to ensuring the safety and resilience of smart cities as they become more prevalent.

Therefore, this study seeks to address this knowledge gap by examining the challenges and issues that hinder the effective implementation of cybersecurity practices in the context of smart Saudi cities. Therefore, as smart cities continue to gain traction in Saudi Arabia, understanding the challenges and issues related to adopting cybersecurity practices becomes vital to ensuring the successful development and operation of these urban environments [10]. Additionally, analyzing the cultural, social, and economic factors that influence the implementation of cybersecurity measures can provide valuable insights into the unique context of Saudi Arabia, which can be used to develop targeted strategies and policies for improving cybersecurity in its smart cities [11]. Finally, the study offers the following research objectives:

1 To identify the challenges and issues in adopting cybersecurity and safety practices by IT professionals and the common public in smart Saudi cities.
2 To explore the economic, social, and cultural factors/challenges that make the cybersecurity framework practicable in smart Saudi cities.
3 To conceptualize a cybersecurity-based UTAUT3 model in smart Saudi cities.

2. Literature Review and Conceptualization

2.1. Challenges and Issues in the Implementation of ICT Technologies

2.1.1. Technological Challenges and Issues

Poor information and communication technology (ICT) infrastructure and security concerns hamper the adoption of e-government in Saudi Arabia. Hosam and Ahmad [12] assert that the lack of ICT infrastructure is a predominant issue. Additionally, there is a need for Saudi Arabia to develop standardized policies and regulations to oversee the use of ICT services. These changes will enable both the government and citizens in delivering services [12]. Privacy and security concerns are another major technical challenge affecting the implementation of cybersecurity in Saudi Arabia. A study by Alshehri and Drew [13]

notes that most Saudi Arabians are concerned that using e-government platform to share personal information, such as names and ID numbers, could expose them to cybersecurity risks. The citizens are afraid that online platforms do not have adequate security to prevent hackers from accessing their data. Regrettably, the concern over the lack of security in e-government systems has created an unwillingness among Saudi Arabians to embrace e-services [13]. Hosam and Ahmad [12] claim that international privacy and security concerns are the leading issues among citizens when using e-government platforms. Thus, the government needs to enhance public awareness of how citizens should safeguard their data and privacy by building cybersecurity practices when using the Internet [12].

2.1.2. Organizational Challenges and Issues

Lack of qualified ICT experts, lack of training, resistance to change, inadequate ICT police, and lack of collaboration between Saudi Arabian agencies are also responsible for the slow adoption of cybersecurity. Alshehri and Drew [13] claim that in Saudi Arabia, most IT experts have moved from the public sector to the private sector since government jobs pay fewer wages compared to corporate jobs. The transition has deprived the public sector of experts who could have helped implement cybersecurity programs [13]. According to Hossam et al. [14], the new phenomenon experiences resistance because people fear the unknown. Since setting cybersecurity in smart cities is an emerging technological revolution in Saudi Arabia, it requires establishing an appropriate framework [12]. For any new government program to succeed, it should receive support from all agencies. Alshehri and Drew [13] claim that Saudi Arabia has experienced slow adoption of cybersecurity measures because of a lack of collaboration between government agencies in promoting their implementation. None of the Saudi Arabian agencies wishes to share their data with other organizations. The country could realize numerous benefits if all the agencies could share their information on cybersecurity practices [13]. These challenges and issues also include:

Lack of Trust

Certain distinctions exist between cybersecurity in Saudi Arabia and the United States. Alotaibi et al. [15] noted that perceived trustworthiness has a positive and major impact on behavioral intention to use m-government services [16]. This observation suggests that most participants in this research trust such applications and their merits since the government has deployed them. This result is consistent with the principle that when trust in the Internet and government is enhanced, the intention to use cybersecurity practices increases. In addition, security may not be a problem for most individuals who adopt security applications since they have been utilizing the Internet for a long time and are well familiar with security and privacy concerns. Privacy issues do not affect the purchase intentions of cloud computing services in the United States [15]. Moreover, they should deliver services through secure applications to motivate users to embrace these technologies [15].

In view of cybercrimes, related regulations in Saudi Arabia are influenced more by Islamic and social principles, as well as local cultural contexts [16]. These laws include the penalties for the different crimes and the fines that the religion considers consistent with the values it practices. During investigations, Saudi Arabia's Communication and IT Commission provides the required technical support to the established security body to assist with the examination of diverse cybercrimes. However, in the United States, the Federal Bureau of Investigation is responsible for investigating such offenses, in line with the Constitution.

Lack of Awareness and Training Developments

In the Middle East region, security awareness of information, particularly among undergraduates, scholarly researchers, and staff, has been examined to determine their degree of knowledge of information systems [17]. In a study, the researchers note that a lack of scholarship on information system principles is the main impediment to cybersecurity

awareness. Several suggestions to minimize the severity of this situation were formulated, namely reinforcing awareness and training initiatives as well as embracing safety measures across learning institutions to promote data security.

Various factors necessitate an examination of cybersecurity in cybersecurity practices. In the view of Saudi Arabia, the e-government paradigm of administrative systems is a relatively new idea, originating in the 1980s. In government contexts, the execution of technology in providing diversified offerings is a costly plan that demands economic practicality. An effective model within which the electorate can access different services is necessary and must be protected to promote social welfare [15]. Given e-government implementation in the country, significant advantages—such as the adoption of digital technologies and a minimization in the cost of public service—have been evident. Saudi Arabia is a nation that maintains a positive outlook on the international stage with the goal of securing varied economic interests [17].

An assessment of Saudi Arabians indicates that their cybersecurity awareness level is considerably low. This situation can be attributed to the nature of the national culture. Additionally, while Saudi citizens exhibit a clear understanding of information technology (IT), their knowledge of cybersecurity risks and the government's role in facilitating information safety across the Internet is quite limited. Therefore, state agencies should create awareness of these issues through training initiatives in learning institutions.

Impacts of Culture

American social customs are broad, coupled with distinct values based on diverse populations and ethnic backgrounds [17]. This convergence means that one religion cannot form the basis for governing the penalties for people found guilty of cybercrime offenses; therefore, a challenge in managing the practice appears [18]. In addition, variations exist in the level of jail time for similar crimes in Saudi Arabia and the United States. Besides, phishing is the most dominant social engineering method in recent times. It entails stealing users' credit card numbers and login details to access their private data. This form of cyberattack accounted for 77% of all social engineering attacks in Saudi Arabia's educational sector in 2017. These attacks can be implemented through the Internet and social media.

Social harmony and human connections are major priorities among Asians. Efficiency and time management, on the other hand, are critical values for Westerners. Such cultural factors have a clear implication for cybersecurity.

Shortage of Local Expertise

In Saudi Arabia, a lack of IT professionals to guide the execution of e-government in their entities is clear [18]. A primary factor for such a lack is the transfer of IT expertise from the public sector to the private sector since government salaries are relatively low [17]. Further, a lack of IT personnel at all levels, including programmers and professional managers, is evident. Consequently, the training of existing employees, especially in the public sector, is vital to advance the adoption of any novel technology. On the other hand, a significant proportion of Saudi Arabia's population lacks the requisite IT competency needed to advance smart cities [17]. Therefore, this situation demands dependence on expatriates to assist in the management of distinct elements of the smart city initiative.

Finally, the study proposes the following assumptions to explore the challenges and issues of adopting cybersecurity practices in smart Saudi cities:

P1. The lack of trust related to cyberinfrastructure issues, services from governments or companies, cyber threat attacks, and a cyber-based economy limit cybersecurity framework adoption in Saudi Arabia.

P2. The lack of developments related to a shortage of cyber awareness programs and a lack of trained personnel limit cybersecurity framework adoption in Saudi Arabia.

P3. Cultural influences, including using social apps, influence Saudi Arabia's adoption of cybersecurity awareness methods.

P4. The lack of IT professionals in the public sector (a shortage of local expertise) limits the implementation of cybersecurity frameworks in Saudi Arabia.

After a careful literature review, the study identified the key challenges for citizens, governments, and organizations in services, mobility, and standards and protocols. Moreover, the study also identified the smart city factors (i.e., privacy, security, and risk) that need proper laws and regulations, wellbeing and quality of life, and governance. Therefore, the study divided all stakeholders (citizens, government, and organizations) into three main factors, including trust, operational and transitional, technological and sustainability challenges. Based on this information, the study also develops a conceptual framework (Figure 1) based on the following proposed propositions:

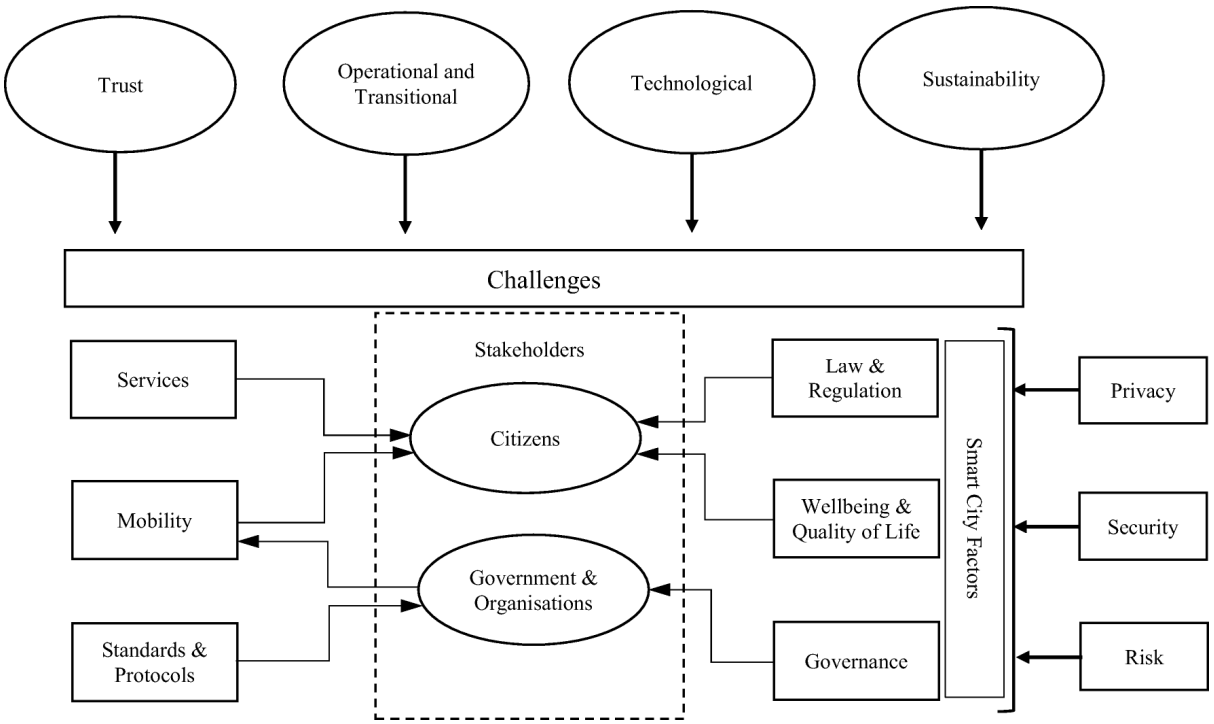

Figure 1. Conceptual framework.

3. Research Methodology

3.1. Research Design

This study adopts a quantitative research method to validate and test the survey items of cybersecurity practices in smart Saudi cities. Quantitative research is focused on collecting and analyzing statistical data, which is suitable for investigating factors in producing repeatable outcomes and generalizing findings [19,20]. Quantitative research is a predominant method due to its objectivity, generalizability, and replicability, as it relies on systematic procedures and numerical data for analysis [21]. Statistical techniques are employed to draw objective conclusions, make inferences about the population, and enhance the rigor and precision of the research. While quantitative research has limitations, such as the potential for overlooking qualitative nuances, its structured and statistical nature makes it accessible and efficient for data collection and analysis. According to the study of cybersecurity in smart cities, the quantitative method has been recommended in previous research [21] to test the assumptions. For this study, a survey-based cross-sectional approach was used to analyze relationships between various factors and the implications of the results for the research approach [19]. Therefore, the study used a survey questionnaire to develop a list of questions about exploring challenges and issues in adopting cybersecurity practices in smart Saudi cities.

3.2. Data Collection Procedure

The study adopted a survey questionnaire technique to collect data. The study collected data from the common public, targeting 710 citizens. The common public was the subject of a survey questionnaire that was distributed in order to collect data. The respondents using an online platform made available to Saudi citizens living in Saudi Arabia used a combined web-based online survey (Google Forms). In order to determine the cybersecurity challenges and issues in smart Saudi cities and the potential benefits they may provide, a literature review was conducted, and a survey questionnaire was created for this research. The survey questionnaire contained only questions that were straightforward, to the point, free of ambiguity, and simple to read. A list of research questions has been developed from an extensive literature review. When the questions were extracted, they were reviewed and proofread by two professors from universities and two IT experts in the same field (cybersecurity). The questionnaire comprised 36 questions identified from reviewing the literature (see Appendix A). A five-point Likert scale was used to measure the items to reduce the possibility of measurement errors and the mental strain placed on the participants [22].

The participants in this research were the public in information technology and cybersecurity (including web designers, software engineers, and programmers). Since Arabic is Saudi Arabia's primary language, but the questionnaire survey was initially written in English, it was necessary to have it translated into Arabic before it could be sent to the common public. Therefore, the study used both versions of the survey questionnaire to allow the common public to respond clearly. According to Sekaran [23], it is vitally important to select a language for the questionnaire that is clear, straightforward, and written at a level that respondents can comprehend. In this particular investigation, the researcher utilized the strategy of back translation. Back translation has recently become increasingly popular for academic translated versions and expert studies.

The designed questionnaire is improved through a process to reduce the number of errors caused by the creation of the questionnaire and ensure that the content is accurate [24]. The study surveyed the public (N = 710) in Saudi Arabia, but only 554 surveys were fully answered, so the study used only completed survey questionnaires. The study surveyed the public to determine the challenges and issues in adopting cybersecurity practices in smart Saudi cities. This strategy elaborates on the responses to the challenges, barriers, and needs of adopting cybersecurity in smart cities in Saudi Arabia. Finally, the study surveyed the public by taking 554 survey responses from two smart cities (for example, Neom and Riyadh) in Saudi Arabia. The researcher used the list of questions to test the assumptions/propositions of the research (see Appendix A).

3.3. Data Analysis

The study used a statistical package for social sciences (SPSS) 21 to analyze the pre-testing survey data [25]. First of all, the study calculated descriptive statistics for the demographic characteristics of the respondents. The study also calculated the correlation coefficient [26] among the variables of the pre-testing survey questionnaire. As well, the study tests the survey questions in order to find the challenges and issues in adopting cybersecurity practices in smart Saudi cities.

4. Results

4.1. Descriptive Statistics (Public Survey)

In Table 1, the descriptive statistics showed that there are 62.8% (348) males and 37.2% (206) females. Moreover, 18.6% (103) of the respondents were from the public sector, 53.6% (297) of the respondents were from the private sector, 2.3% (13) of the respondents were unemployed, 9.2% (51) of the respondents were housewives, construction employees, teachers, medical doctors, or military men, 9.6% (53) of the respondents were students, and 6.7% (37) of the respondents were from free businesses. Additionally, 33% (183) of the respondents were using fast internet, 48.2% (267) of the respondents were using medium-

speed internet, 15% (83) of the respondents were using low internet, and only 3.8% (21) of the respondents were using very fast speed internet.

Table 1. Frequency and percentage of the participants of the study (N = 554).

Gender	Frequency	Percent	Valid Percent	Cumulative Percent
Male	348	62.8	62.8	62.8
Female	206	37.2	37.2	100.0
Total	554	100.0	100.0	
Occupation				
Public sector	103	18.6	18.6	18.6
Private sector	297	53.6	53.6	72.2
Unemployed	13	2.3	2.3	74.5
Others (housewife, construction, teacher, medical, military)	51	9.2	9.2	83.8
student	53	9.6	9.6	93.3
Free business	37	6.7	6.7	100.0
Total	554	100.0	100.0	
How do you rate your current internet speed				
Fast	183	33.0	33.0	33.0
Medium	267	48.2	48.2	81.2
Slow	83	15.0	15.0	96.2
Very fast	21	3.8	3.8	100.0
Total	554	100.0	100.0	

4.2. Correlation Analysis

The strength and degree of the linear links between two sets of variables are evaluated using correlation coefficients. Therefore, the study used correlation analysis to check the relationship between the variables. Table 2 describes the correlation analysis of the factors related to the Internet and cybersecurity. The results showed that internet services are positively and strongly associated with the latest technologies (r = 0.406 **) and increased cybersecurity issues (r = 0.122 **). In addition, it was also observed that cybersecurity issues are significantly and positively related to the development of the latest technology (r = 0.092 *) and electronic services information (r = 0.099 *). At the same time, no significant relationship was observed between electronic services and cybersecurity scams (r = −0.071), and the relationship was negative. Finally, it was proven that there was the highest correlation coefficient between internet services and the latest internet technology. It happened due to the notion that if there is the latest internet technology, the use of internet services will increase automatically.

Table 2. Correlation coefficients (N = 554).

Correlations	*Internet Services*	*Latest Internet Technology*	*Cybersecurity Scam*	*Electronic Services Information*
Internet services	-	0.406 **	0.122 **	−0.028
Latest internet technology	-	-	0.092 *	0.099 *
Cybersecurity scam	-	-	-	−0.071
Electronic services information	-	-	-	-
**. Correlation is significant at the 0.01 level (2-tailed).				
*. Correlation is significant at the 0.05 level (2-tailed).				

Note: ** $p < 0.01$, * $p < 0.05$.

4.3. Testing Assumptions

4.3.1. Lack of Trust

The survey results indicate that there needs to be more trust in cyber infrastructure and the digital economy in Saudi Arabia (Table 3). A majority of respondents believe that the country has weak cybersecurity platforms, and they need more confidence in the nation's capacity to design and deploy smart cities. Despite this, many participants acknowledge the country's shift towards a digital economy. The respondents display awareness of various IT issues, such as social media scams, bank fraud, and fake advertisements. Concerns about external threats, fake accounts, information leakage, hacking, and improper cybersecurity systems are prevalent. Most participants have experienced medium or slow internet speeds, and many have faced security or privacy breaches. Furthermore, the majority of respondents admit to sharing their personal information online without reading the website's privacy policy. These findings suggest that cybersecurity and digital infrastructure improvements are crucial to increasing trust and confidence in Saudi Arabia's technological advancements.

Table 3. Lack of trust.

Lack of Trust (Cyber Infrastructure)		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Does Saudi Arabia have good cybersecurity platform?		1 (1%)	2 (1.9%)	20 (19%)	45 (42.9%)	35 (33.3%)
How strongly believe we have knowledge and capacity to design and deploy smart cities?		0	5 (4.8%)	31 (29.5%)	32 (30.5%)	35 (33.3%)
Lack of trust (digital economy)						
Rate how much Saudi Arabia is moving towards digital economy?		71 (67.6%)	25(23.8%)	4 (3.8%)	3 (2.9%)	
Awareness about various IT issues						
Email scam						2 (1.94%)
Bank fraud						5 (4.85%)
Social media scam						30(29.12%)
Viruses (that can lose the personal information from the workplace)						15 (14.56%)
Mobile data						14 (13.59%)
Fake advertisements (job advertisement, links on social media, advertisement messages)						20 (19.41%)
Trust and continuity competition						
External threats						8 (7.76%)
Fake accounts or hackers						9 (8.73%)
						Frequency
Information leakage						23 (22.33%)
Hacking bank accounts						22(21.35%)
Unprofessional work environment						27 (26.21%)
Improper cybersecurity system						31 (30.09%)
Use of smart devices based on internet speed			Are you aware of your internet-connected smart devices at home?			
			No			Yes
How do you rate your current internet speed?	Fast		5 (13.88%)			178 (34.36%)
	Medium		22 (61.11%)			245 (47.29%)
	Slow		9 (25%)			74 (14.28%)
	Very fast		0(0%)			21 (4.05%)
	I don't know		No			Yes
Have you had any problems with breaching security/privacy?	I haven't had problems breaching security/privacy, and I'm not worried about these issues.		5 (18.51%)	74 (16.26%)		5 (6.94%)
	I haven't had problems breaching security/privacy, but I worry about these issues.		18 (66.6%)	344 (75.60%)		40 (55.5%)
	I've recently had problems breaching security/breaching privacy, and I'm concerned about these issues.		4 (14.81%)	37 (8.13%)		27 (37.5%)
			Do you realize that you share your personal information with e-government services?			
			No	Yes		
Have you shared your phone number or personal information online without reading the website's privacy policy?	No		44 (17.39%)	209 (82.60%)		253
	Yes		48 (15.94%)	253 (84.05%)		301
Total			92	462		554

4.3.2. Lack of Awareness and Training Developments

The majority of Saudi citizens surveyed believe it is essential to be aware of cyber threats, with 74% strongly agreeing and 20.2% agreeing. A considerable percentage (40%) of respondents have already participated in a cybersecurity community awareness program, demonstrating an overall interest in the topic. Furthermore, an overwhelming majority

(97.09%) expressed interest in promoting a cyber-awareness program within the community, should the government provide incentives. Regarding participating in training, a higher proportion of respondents (62.68%) are willing to pay a small fee for the course, as opposed to 37.3% who would prefer not to pay. In conclusion, the findings indicate that Saudi citizens are highly aware of the importance of cyber threats and demonstrate a significant willingness to participate in and promote cybersecurity awareness programs, with a majority also being open to paying for relevant training courses.

Most participants recognize the importance of cyber threat awareness, indicating a successful initial stage of cybersecurity education and potential readiness for more in-depth knowledge. Despite the recognized importance of awareness, participation in cybersecurity community awareness programs could be much higher. This highlights a gap between understanding the importance of cyber awareness and taking active steps to increase it. Most participants would be interested in promoting cyber-awareness programs if the government provided incentives. This reveals a significant opportunity for government agencies to boost cybersecurity education through incentivized initiatives.

Participants' willingness to pay for a course indicates a market for paid cybersecurity education. However, only some interested people are willing to pay, suggesting that affordable or free training options might be necessary to reach a wider audience. While most interested participants are eager to invest financially in their cybersecurity education, many uninterested participants would not pay for such a course. This suggests that financial commitment may deter some individuals, necessitating additional strategies to engage this group, such as demonstrating the practical benefits of such training (Table 4).

Table 4. Lack of awareness and training developments.

Awareness of Cyber Threats	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
How strongly you think it is good to have every Saudi citizen to be aware of Cyber threats?	0	1 (1%)	4 (3.8%)	21 (20.2%)	77 (74%)
Willingness to participate in cybersecurity awareness program		Yes		No	
Have you participated in cybersecurity community awareness?		42 (40%)		61 (58%)	
Variable		Yes		No	
Will you be interested in promoting cyber-awareness program to community, if the government provides some incentive for you?		100 (97.09%)		3 (2.91%)	
Interest and willingness to participate in trainings		No		Yes	Total
Are you ready to pay a small fee for the course?	No	159 (49.22%)		75 (37.3%)	234
	Yes	194 (54.95%)		126 (62.68%)	320
Total		353		201	554

4.3.3. Impact of Culture

The survey results indicate that a significant proportion of respondents believe that advancements in IT infrastructure will impact Saudi culture, with 14.3% strongly agreeing and 32.4% agreeing on this issue (Table 5). However, a notable percentage (40%) remain neutral, while 6.7% disagree and 4.8% strongly disagree. In terms of social apps affecting Saudi culture, Snapchat (51.4%) and Twitter (32.4%) are identified as the two most influential apps, with WhatsApp (14.3%) coming in third place and no respondents selecting Instagram or other apps. In conclusion, most respondents believe that advancements in IT infrastructure and the use of social apps, notably Snapchat and Twitter, have the potential to affect Saudi culture. However, a considerable portion remains neutral on the topic.

Table 5. Impacts of culture.

Impacts of Culture	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Do you believe advancement in IT infrastructure will affect the Saudi culture	15 (14.3%)	34 (32.4%)	42 (40%)	7 (6.7%)	5 (4.8%)
Social apps affecting Saudi culture	Twitter	Snapchat	WhatsApp	Instagram	Others
34. Provide two important technology apps (social apps) that affect Saudi culture.	34 (32.4%)	54 (51.4%)	15 (14.3%)	0	0

4.3.4. Shortage of Local Expertise

The survey results reveal that only a small percentage (11.4%) of respondents have the technical ability to perform network-wide deep-packet inspections (Table 6). In comparison, a more significant portion (41%) do not have this capability, and 45% are uncertain. There is a generally positive outlook regarding job satisfaction and the potential of public and governmental agencies to match private sectors shortly, with 36.2% strongly agreeing and 36.2% agreeing with the statement. However, 19% of respondents remain neutral, while 3.8% disagree, and 2.9% strongly disagree. In conclusion, although the technical ability to perform deep-packet inspections is limited among the respondents, there is optimism that public and governmental agencies can match private sectors shortly.

Table 6. Shortage of local expertise.

Technical Ability of IT Specialists			**Yes**	**No**	**I Don't Know**
Do you have the technical ability to perform network-wide deep-packet inspections?			12 (11.4%)	43 (41%)	48 (45%)
Job satisfaction	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
How strongly you agree with the following statement: Public sector and governmental agencies can match private sectors in the new future:	(36.2%)	(36.2%)	(19%)	(3.8%)	(2.9%)

5. Conceptualization of the Cybersecurity-Based UTAUT Model

After identifying the challenges and gaps in the survey, it is shown that other economic, cultural, and social factors are related to behavioral intention and actual use of behavior. The literature review showed that economic, cultural, and social factors significantly contribute to behavioral intention and the actual behavior of using smart city technologies. The study identified several factors from the literature studies and tested the results. The factors for each antecedent are termed economic factors, i.e., privacy design (safety), cyber threat intelligence and analysis platform (resiliency); social factors, i.e., digital trust (confidentiality), cyber responses and resilience (availability); and cultural factors, i.e., cyber competencies and awareness program (integrity).

The study used the unified theory of acceptance and use of technology (UTAUT) as the basis to develop a cybersecurity-based UTAUT3 model in smart Saudi cities. Popova and Zagulova [27] in the smart city of Riga, Latvia, use UTAUT models in predicting cybersecurity behaviors and intentions, such as in a study. The study findings showed that all factors of the UTAUT model (i.e., performance expectancy, effort expectancy, social influence, and facilitating conditions) significantly contributed to the behavioral intention and actual use of behavior in adopting smart city technologies. However, they claimed that UTAUT factors might not predict adopting smart city technologies due to the underdeveloped culture. Kuberkar and Singhal [28] conducted a study by testing the behaviors of passengers toward smart city transport technologies. The study stated that performance expectancy, effort expectancy, social influence, facilitating conditions, trust, and anthropomorphism affect behavioral intention and actual use of behavior in adopting smart city transport technologies. Meanwhile, Van Zoonen [29] recognized security and privacy as contributing factors in the smart city awareness campaign model, in which privacy and security variables are connected to applying the appropriate realm of the smart city.

In this context, some of the issues include developing resilience in information security; increasing awareness of privacy risks; growing the security and integrity of online content, thereby encouraging greater use of information systems [30]; generating policy standards for cybersecurity based on global best practice; constructing resilient information systems; and increasing concern regarding security risks [17]. Alzahrani [31] conducted a study claiming that cybersecurity's availability, confidentiality, and integrity are linked to cybersecurity trust and culture. It is helpful to increase the safety of critical systems and cyber resilience capability, conduct research and training, and market cybersecurity remedies, products, or services when government organizations and commercial sectors

engage. Therefore, Alzahrani [31] stated that data availability, confidentiality, and integrity should be enhanced to cover the lack of system development and IT experts. On the other hand, Alhalafi and Veeraraghavan [32] proposed recommendations for Saudi Arabia to implement a cybersecurity framework for smart cities. They claimed that smart cities require a model of cybersecurity that will safeguard their integrity and guide the reaction to possible assaults and hazards [32]. Based on the study's findings and evidence in the literature, the study develops a cybersecurity-based UTAUT3 model in smart Saudi cities (see Figure 2):

Figure 2. Conceptual framework 2.

6. Research Methodology

6.1. Data Collection Procedure

The questionnaire was developed based on the findings of the previous survey conducted in smart Saudi cities. The configuration of the research questionnaire uses an online platform, which details the study's objectives and provides the researcher and the supervisors' team with their respective contact information. On the cover page, which was explicitly designed to inform the respondents of the objectives and significance of this research, the researcher provided an explanation of the objectives of the survey and directions for completing the questionnaire at the start of the study. The questionnaire was designed to validate the conceptual framework in smart Saudi cities using nine factors. An emphasis was placed on the nine factors of the UTAUT3 model (performance expectancy, effort expectancy, social influence, facilitating conditions, safety, resiliency, availability, confidentiality, and integrity of cybersecurity) that had been taken. The questionnaire is

divided into two distinct sections. Respondents' demographic data were gathered in the first part of the survey. The second section of the questionnaire consisted of UTAUT3 factors and items to validate the cybersecurity-based UTAUT3 model. The survey questionnaire validity and reliability testing involved the researcher sending the questionnaire to five scientists who are currently pursuing their doctoral degrees and have substantial expertise in cybersecurity and e-applications, in addition to having a solid understanding of Arabic, which is also their native language. The questionnaire was written in English and Arabic. The feedback from the doctoral students recommended minor alterations to the wording; furthermore, the feedback suggested splitting up a few questions and evolving the order in which they were asked. Their feedback was incorporated into the revision of the draft questionnaire, and then the completed survey instrument was presented to them and received their approval. Finally, a second survey consisting of 108 IT professionals was carried out for the purpose of validating the conceptual model.

6.2. Measurement Scales

This study's assessment constructs and items were derived from previous research (see Appendix B). Four performance expectancy items, three effort expectancy items, three social influence items, and three facilitating conditions items were gathered from earlier studies and modified for this investigation [33,34]. Based on Arpaci and Sevinc's [35] research, the study adapted the following cybersecurity factors: four safety items, three resilience items, three secrecy items, three availability items, and four integrity items. Additionally, the research adjusted three items of behavioral intention and three items of actual use behavior from past studies to facilitate data comparison [33,34]. A Likert scale was employed for the measurement scales, with levels ranging from 1 (strongly disagree) to 5 (strongly agree). McDaniel and Gates [36] argue that a Likert scale is practical when the research measures participants' attitudes towards various factors.

6.3. Data Analysis

This stage of the survey questionnaire was conducted to develop and validate the factors of the UTAUT3 cybersecurity framework in smart Saudi cities. The study used the Smart PLS 3.3.3 version to develop and validate the new UTAUT3 cybersecurity framework in smart Saudi cities. The study used the first step of the algorithm technique to assess the measurement model. The research-based guidelines of previous researchers in the literature have been followed in this research [37,38] to assess and test the research-developed conceptual framework.

7. Validation and Development of Cybersecurity-Based UTAUT3

7.1. Demographic Information

The demographic information of the pre-test shows that 50% (54) of the respondents were from the IT sector, 19.4% (21) of the respondents from the education sector, only 7.4% (8) from the construction sector, and 23.1% (25) of the respondents from the food sector. The study also reported that 71.3% (77) of the respondents were male and 28.7% (28.7) were female. Meanwhile, the study reported that 15.7% (17) of the respondents have 1–2 years of IT experience, 13% (14) of the respondents have 2–5 years of IT experience, 32.4% (35) of the respondents have 5–8 years of experience, 15.7% (17) of the respondents have 8–10 years of experience, and 23.1% (25) of the respondents have 10+ years of experience. On the other hand, the study finds that only 8.3% (9) of the respondents have matriculation education, 54.6% (59) of the respondents have intermediate education, 34.3% (37) of the respondents have a bachelor's degree, 1.9 (2) of the respondents have a master's degree, and 0.9% (1) of the respondents have a Ph.D. degree.

7.2. Convergent Validity and Reliability

The convergent validity and reliability of the measurement scales can be assessed using the threshold values established in the literature [39–41]. Convergent validity is

demonstrated when all factor loadings are greater than 0.7 [41] and the average variance extracted (AVE) is greater than 0.5 [42]. Reliability is established when both Cronbach's alpha and composite reliability (CR) values are greater than 0.7 [39,40]. The study ran an algorithm with 5000 sub-samples and found that two items of facilitating conditions (FC1 = 0.446, FC2 = 0.508), one item of safety (SAFE4 = 0.626), one item of confidentiality (CON1 = 0.638), and one item of availability (AVAI2 = 0.655) have lower factor loading than 0.7, so they have been deleted from the model. In this study, all measurement scales show satisfactory convergent validity and reliability, as all factor loadings are above the 0.7 threshold, and AVE values for each scale exceed 0.5 (Table 7). Moreover, Cronbach's alpha and CR values are greater than 0.7 for all scales, indicating high internal consistency and reliability (Table 7).

Table 7. Convergent validity and reliability.

Measurement Scales	Items	Factor Loadings	AVE	Cronbach Alpha	Composite Reliability
Actual use of behavior	AUB1	0.837	0.704	0.790	0.877
	AUB2	0.822			
	AUB3	0.858			
Availability of cybersecurity	AVAI1	0.746	0.641	0.719	0.842
	AVAI3	0.794			
	AVAI4	0.858			
Behavioral intention	BI1	0.780	0.651	0.735	0.848
	BI2	0.840			
	BI3	0.799			
Confidentiality of cybersecurity	CON2	0.833	0.748	0.831	0.899
	CON3	0.887			
	CON4	0.874			
Effort expectancy	EE1	0.852	0.670	0.753	0.859
	EE2	0.803			
	EE3	0.799			
Facilitating conditions	FC3	0.753	0.644	0.725	0.844
	FC4	0.797			
	FC5	0.854			
Integrity of cybersecurity	INT1	0.798	0.643	0.815	0.878
	INT2	0.852			
	INT3	0.752			
	INT4	0.803			
Performance expectancy	PE1	0.824	0.628	0.803	0.871
	PE2	0.769			
	PE3	0.785			
	PE4	0.792			
Resiliency of cybersecurity	RESI1	0.811	0.662	0.746	0.855
	RESI2	0.810			
	RESI3	0.821			
Safety of cybersecurity	SAFE1	0.888	0.679	0.841	0.894
	SAFE2	0.810			
	SAFE3	0.837			
	SAFE5	0.756			
Social influence	SI1	0.789	0.717	0.803	0.884
	SI2	0.862			
	SI3	0.887			

7.3. Discriminant Validity

Cross-loadings are the correlation coefficients between the items and the factors, and they are used to evaluate the discriminant validity of the measurement scales [39]. Discriminant validity is established when the items load higher on their respective factors than on others [43]. A common rule of thumb is that the difference between the item's loading on its own factor and its highest loading on other factors should be at least 0.1 [43]. The findings showed that most items have a higher loading on their respective factors (diagonal elements in bold) than on other factors (off-diagonal elements). This suggests a reasonable level of discriminant validity for most of the items in this study (see Appendix C).

Another part of discriminant validity is testing the Fornell–Larcker [44] criterion. The Fornell–Larcker criterion is an approach used to assess discriminant validity, which is the

degree to which a construct is distinct from other constructs [44]. This criterion is fulfilled when the square root of a construct's average variance extracted (AVE) is greater than the correlations between that construct and all other constructs in the model. In Table 8, the diagonal values (in bold) represent the square root of AVEs for each construct, while the off-diagonal values represent the correlations between the constructs. Based on the Fornell–Larcker criterion, it can be concluded that discriminant validity is established for most of the constructs as the square root of the AVE for each construct is higher than its correlations with other constructs.

Table 8. Fornell–Larcker criterion.

Factors	1	2	3	4	5	6	7	8	9	10	11
Availability of cybersecurity	**0.801**										
Behavioral intention of adopting cybersecurity in smart cities	0.548	**0.807**									
Confidentiality of cybersecurity	0.631	0.428	**0.865**								
Effort expectancy	0.373	0.564	0.373	**0.819**							
Facilitating conditions	0.542	0.609	0.462	0.640	**0.802**						
Integrity of cybersecurity	0.474	0.574	0.342	0.560	0.555	**0.802**					
Performance expectancy	0.538	0.510	0.317	0.493	0.680	0.440	**0.793**				
Resiliency of cybersecurity	0.534	0.651	0.501	0.559	0.606	0.619	0.523	**0.814**			
Safety of cybersecurity	0.505	0.644	0.470	0.581	0.638	0.621	0.501	0.725	**0.824**		
Social influence	0.376	0.531	0.340	0.693	0.551	0.546	0.459	0.531	0.501	**0.847**	
Use behavior of adopting cybersecurity in smart cities	0.455	0.733	0.407	0.508	0.589	0.654	0.450	0.677	0.762	0.551	**0.839**

7.4. Model Fitness (R-Square)

R-square (R^2) measures the proportion of variance in the dependent variable that the independent variables can explain in a multiple regression model. It is a commonly used statistic to evaluate the goodness of fit of a model. R-square values range from 0 to 1, with higher values indicating a better fit between the model and the data [39]. In the given study, the R^2 values for the two dependent variables, behavioral intention of adopting cybersecurity in smart cities and use behavior of adopting cybersecurity in smart cities, are 0.567 and 0.537, respectively. These values suggest that the nine factors in the model explained 56.7% of the variance in behavioral intention and 53.7% of the variance in user behavior.

8. Discussion and Conclusions

The existing literature and studies underscore the significant influence of economic, cultural, and social factors on the behavioral intention and actual use of smart city technologies. Applying the unified theory of acceptance and use of technology (UTAUT) to cybersecurity contexts, particularly in smart cities, has yielded significant findings concerning performance expectancy, effort expectancy, social influence, and facilitating conditions. However, gaps in cultural development and specific factors such as privacy, security, trust, and anthropomorphism were also identified as critical aspects of technology adoption. Emphasizing the need for resilient information systems and raising awareness of privacy and security risks are pivotal steps toward strengthening smart city infrastructure. Therefore, factors including data availability, confidentiality, and integrity are addressed to mitigate the dearth of system development and IT expertise. Consequently, developing and implementing a comprehensive cybersecurity framework is paramount to safeguarding the integrity of smart cities, providing guidance for respoding to potential threats, and promoting a robust and secure digital environment. After that, this study examines the widespread phenomenon of testing the behavioral intentions in adopting cybersecurity awareness programs in two cities in Saudi Arabia (i.e., Riyadh and Neom). The study

conducted two surveys. The first survey was carried out to explore the challenges and issues in adopting cybersecurity practices in smart Saudi cities. The second survey was carried out to develop and validate the conceptual cybersecurity-based UTAUT3 model. In the first phase, the study targeted 554 respondents (common public). In the second phase, the study targeted 108 IT professionals because they provided the most authentic responses to validate a new model in smart Saudi cities. The survey results reveal several key insights about trust in cyberinfrastructure and the digital economy in Saudi Arabia. First, there is a widespread perception of weak cybersecurity platforms and a need for more confidence in the country's ability to design and deploy smart cities. Second, respondents are highly aware of various IT issues and have experienced security or privacy breaches. Third, Saudi citizens understand the importance of cyber threats and express a strong interest in participating in cybersecurity awareness programs. Furthermore, most respondents believe that advancements in IT infrastructure and social apps, notably Snapchat and Twitter, have the potential to impact Saudi culture. However, a considerable portion of respondents remains neutral on this issue. While technical abilities such as deep-packet inspections are limited among the respondents, there is optimism that public and governmental agencies can match the private sector shortly.

The study results emphasize the importance of economic, cultural, and social factors in shaping behavioral intention and actual use of smart city technologies. Key factors identified include privacy design, cyber threat intelligence, digital trust, cyber responses, resilience, and cyber competencies and awareness programs. Moreover, the R^2 values of 0.567 and 0.537 for behavioral intention and user behavior, respectively, indicate that the nine factors (performance expectancy, effort expectancy, social influence, facilitating conditions, safety, resiliency, confidentiality, availability, and integrity of cybersecurity) in the cybersecurity-based UTAUT3 model explain a significant proportion of the variance in these two dependent variables. This suggests that a comprehensive approach addressing economic, social, and cultural factors is crucial for increasing trust in cyberinfrastructure and promoting the adoption of cybersecurity measures in smart cities within Saudi Arabia.

Combining the two surveys' findings, the study concludes by emphasizing the interconnectedness of public perception, technical abilities, and the role of economic, social, and cultural factors in influencing the adoption of cybersecurity measures in Saudi Arabia's transition to a digital economy and smart cities. Additionally, the results highlight the need for effective government policies, incentives, and awareness programs to enhance the overall trust and confidence in the country's cyber infrastructure and digital advancements. The findings of the study presented cybersecurity aspects and factors, including the actual use of behavior, availability, behavioral intention, confidentiality, effort expectancy, facilitating conditions, integrity, performance expectancy, resiliency, safety, and social influence in the context of smart cities. These were each measured with several items, which resulted in factor loadings ranging from 0.746 to 0.888, indicating a high level of validity and reliability. Moreover, all constructs scored above 0.6 in average variance extracted (AVE), implying good convergent validity. Furthermore, all constructs' Cronbach alpha and composite reliability values were above the acceptable 0.7 thresholds, indicating high reliability and internal consistency. The correlation matrix noted that all the constructs were significantly correlated with each other, ranging from 0.317 to 0.733, with the diagonal showing the square root of AVE, illustrating adequate discriminant validity. This indicates that the constructs are related yet distinct from each other, thereby supporting the validity and reliability of the scales used in measuring these constructs. These measurements could be instrumental in shaping cybersecurity policy and best practices in the context of smart cities.

8.1. Practical Implications

The practical implications of this study, which focuses on developing and applying a cybersecurity-based UTAUT3 model in smart Saudi cities, are manifold. Implementing this model can lead to several changes in cybersecurity practices, including the following:

1. **Enhanced understanding of user adoption factors:** The UTAUT3 model provides a comprehensive framework for understanding the factors influencing the adoption of cybersecurity measures in smart cities. By identifying key economic, social, and cultural factors, policymakers and city planners can develop targeted strategies to increase trust and confidence in cyberinfrastructure and promote the adoption of advanced security measures.
2. **Improved cybersecurity awareness programs:** The UTAUT3 model emphasizes the importance of cyber competencies and awareness programs in shaping users' behavioral intentions and actual use of cybersecurity measures. By designing and implementing effective cybersecurity awareness campaigns, government agencies can equip citizens with the necessary knowledge and skills to identify, prevent, and respond to cyber threats.
3. **Informed policy development:** Understanding the factors influencing the adoption of cybersecurity measures in smart cities can help policymakers develop informed strategies that address economic, social, and cultural barriers. This may include providing incentives for participating in cyber-awareness programs, supporting training and education initiatives, and fostering public–private partnerships to improve cyberinfrastructure.
4. **Strengthened cybersecurity practices:** By addressing the concerns and needs of users, as identified in the UTAUT3 model, smart cities can design and deploy robust cybersecurity platforms that address privacy, resiliency, confidentiality, availability, and integrity. This will result in a more secure digital environment, fostering trust and confidence among citizens.
5. **Promoting digital trust and collaboration:** By addressing the concerns and needs of users in smart cities, the UTAUT3 model can help build digital trust among citizens, businesses, and government agencies. This will encourage greater collaboration in developing and maintaining cybersecurity practices, ultimately leading to more secure and resilient smart cities.
6. **Preserving cultural values:** The UTAUT3 model considers the potential impact of IT infrastructure advancements on Saudi culture. By considering these cultural factors, policymakers and city planners can ensure that cybersecurity practices align with societal values and contribute positively to the overall development of smart cities.

8.2. Limitations and Future Directions

While the study provides valuable insights into the factors influencing cybersecurity practices in smart Saudi cities, it has some limitations. The sample size and demographic distribution of respondents may only represent part of the population, potentially limiting the generalizability of the findings. The most significant limitation of the study is that it developed and validated the cybersecurity-based UTAUT3 model but did not examine the effect of all nine factors on behavioral intentions and actual use of behavior in adopting cybersecurity practices; a future study should consider this aspect to investigate the impacts. Furthermore, the study focuses solely on Saudi Arabia, and the results may not directly apply to other countries or regions with different cultural, economic, and social contexts. Future research could address these limitations by employing more extensive and diverse samples and conducting comparative studies across multiple regions or countries. Additionally, researchers could explore the long-term effects of implementing the UTAUT3 model on the overall security and resilience of smart cities, examine the role of emerging technologies such as artificial intelligence and blockchain in enhancing cybersecurity, and investigate the impact of evolving cyber threats on user behavior and adoption patterns.

Author Contributions: N.A. and P.V. contribute to saudi smart cities to identify the challenges and issues in adopting cybersecurity practices. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Study data cannot be shared due to ethical considerations.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Survey Items

Demographic Information					
Gender					
Male			Female		
Occupation					
Public sector	Private sector	Unemployed	Others (housewife, construction, teacher, medical, military)	Student	Free business
How do you rate your current internet speed?					
Slow	Medium	Fast	Very Fast		
Proposed questions based on assumptions					
Lack of Trust					
1.	Does Saudi Arabia have a good cybersecurity platform?				
2.	Does Saudi Arabia have a good cybersecurity platform?				
3.	How strongly believe we have the knowledge and capacity to design and deploy smart cities?				
4.	Rate how much Saudi Arabia is moving towards digital economy?				
5.	What is the most important concern that you may face while using the Internet?				
6.	The major parameter of lack of trust on cyber infrastructure				
7.	How do you rate your current internet speed?				
8.	Are you aware of your internet-connected smart devices at home?				
9.	Do you know about the digital economy?				
10.	Have you ever made any transactions online (e.g., paying an online bill, shopping, etc.)?				
11.	Have you had any problems with breaching security/privacy?				
12.	Has your card been subjected to any fraud?				
13.	Have you shared your phone number or personal information online without reading the website's privacy policy?				
14.	Do you realize that you share your personal information with e-government services?				
15.	Have you clicked on any electronic links you have received via SMS, anonymous WhatsApp messages, email, or any other anonymous media?				
16.	What is Saudi Arabia's shift towards e-commerce?				
17.	Would you like to participate in an e-commerce training course?				
18.	Do you think e-commerce will be a good alternative to traditional trade?				
19.	Do you expect e-commerce to have a successful future in Saudi Arabia over the next five years?				

Lack of awareness and training developments	
1.	How strongly do you think it is good to have every Saudi citizen to be aware of Cyber threats?
2.	Have you participated in cybersecurity community awareness?
3.	Will you be interested in promoting cyber-awareness program to the community, if the government provides some incentive for you?
4.	How strongly do you agree with this statement: Keeping personal and identifiable information safe and secure is at most priority.
5.	How satisfied are you if we give you benefits and incentives when you serve the community?
6.	How satisfied are you if given a chance in a competitive program with special privileges?
7.	Do you know anything about cybersecurity?
8.	Do you think it's important to learn the basics of the concept of cyberattacks?
9.	Are you interested in attending an awareness course on cybersecurity or any course on security?
10.	Do you know the basics of using technology?
11.	Are you ready to pay a small fee for the course?
12.	Have you ever participated in a technology training course?
Impacts of culture	
1.	Do the citizens of Saudi Arabia want to live in a Smart digital city?
2.	To your knowledge, what percentage of Saudi citizens are not aware of current cyber threats?
3.	Do you believe advancement in IT infrastructure will affect the Saudi culture?
4.	Provide two important technology apps (social apps) that affect Saudi culture.
5.	Would you like to live in a smart digital city?
6.	Are you aware of the terms of smart cities?
Shortage of Local Expertise	
1.	Do you have the technical ability to perform network-wide deep-packet inspections?
2.	Preference for working in the private sector?
3.	Reasons for working in the private sector
4.	Reasons to avoid working in the public sector.
5.	How strongly do you agree with the following statement: Public sector and governmental agencies can match private sectors in the new future

Appendix B. Survey Items

Measurement Scales
Actual use of behavior in adopting cybersecurity in smart cities
I use cybersecurity in smart cities frequently during my job period
I use many functions of cybersecurity in smart cities
I depend on cybersecurity in smart cities.
Availability of cybersecurity
I use an up-to-date antivirus program on my devices.
I keep the firewall installed on my devices turned on.
I do not open the files I downloaded from the Internet without scanning with an anti-virus program.
Behavioral intention in adopting cybersecurity in smart cities
I intend to continue using cybersecurity in smart cities.
For my smart city, I would use cybersecurity.
I will continue to use cybersecurity on a regular basis.
Confidentiality of cybersecurity
I do not share information and documents in smart city cyberspace that I do not want to share with third parties in real life.
I ensure that the necessary people can only view the data I share in smart city cyberspace.
I do not share my contact information in smart city cyberspace.
Effort expectancy
I find cybersecurity technologies clear and easy to use.
I have the skills I need to use the cybersecurity technologies in my city.
Learning to operate and use new cyber technologies is easy for me.
Facilitating conditions
My technical support team are experts in their fields and they support cybersecurity very well in my city
Technical support is important for cybersecurity usage and it facilitates my work
A specific person (or group) is available for assistance with cybersecurity in smart cities.
Integrity of cybersecurity
It is safe to store data in smart city cyberspace.
Information and documents I have stored in smart city cyberspace are not lost or deleted.
Sharing data in smart city cyberspace does not involve any risk.
Information and documents stored in smart city cyberspace cannot be accessed by third parties.
Performance expectancy
I find cybersecurity technologies useful for smart cities.
Using cybersecurity technologies enables me to accomplish tasks more quickly.
Cybersecurity increases communication between IT professionals and citizens.
Using cybersecurity technologies makes it easier to protect smart cities
Resiliency of cybersecurity
I tend to bounce back quickly after hard times in cybersecurity
It does not take me long to recover smart protection from a stressful event
I usually come through difficult times with little trouble due to cybersecurity
Safety of cybersecurity
I use the correct cybersecurity safety for carrying out smart city projects
I ensure the highest levels of cybersecurity safety when I carry out smart city projects
I voluntarily carry out tasks or activities that help to improve cybersecurity safety
I help my coworkers when they are working under risky or hazardous Conditions on small city projects
Social influence
The supervisor thinks that I should use cybersecurity for smart cities.
My colleagues have helped me to use cybersecurity technologies in smart cities.
Most staff in my IT department think cybersecurity for smart cities is important

Appendix C. Cross-Loadings

	1	2	3	4	5	6	7	8	9	10	11
AUB1	0.406	0.645	0.470	0.427	0.556	0.429	0.412	0.541	0.632	0.485	0.837
AUB2	0.366	0.595	0.210	0.366	0.380	0.606	0.293	0.530	0.677	0.352	0.822
AUB3	0.372	0.601	0.332	0.485	0.543	0.620	0.423	0.635	0.610	0.548	0.858
AVAI1	0.746	0.426	0.695	0.438	0.511	0.459	0.456	0.545	0.497	0.365	0.422
AVAI3	0.794	0.404	0.464	0.241	0.376	0.313	0.364	0.283	0.402	0.212	0.328
AVAI4	0.858	0.481	0.375	0.224	0.416	0.368	0.467	0.447	0.326	0.320	0.347
BI1	0.307	0.780	0.154	0.428	0.373	0.420	0.274	0.422	0.433	0.349	0.536
BI2	0.464	0.840	0.421	0.548	0.588	0.485	0.523	0.599	0.663	0.579	0.690
BI3	0.545	0.799	0.432	0.369	0.486	0.481	0.402	0.535	0.426	0.318	0.524
CON2	0.478	0.387	0.833	0.378	0.484	0.348	0.387	0.384	0.454	0.247	0.346
CON3	0.653	0.377	0.887	0.310	0.382	0.244	0.230	0.490	0.357	0.310	0.352
CON4	0.504	0.344	0.874	0.274	0.321	0.294	0.195	0.425	0.407	0.328	0.357
EE1	0.275	0.455	0.269	0.852	0.564	0.398	0.453	0.396	0.463	0.554	0.345
EE2	0.286	0.473	0.247	0.803	0.494	0.402	0.322	0.426	0.427	0.554	0.418
EE3	0.355	0.455	0.402	0.799	0.515	0.577	0.438	0.550	0.538	0.594	0.483
FC3	0.421	0.401	0.312	0.461	0.753	0.405	0.541	0.380	0.317	0.359	0.374
FC4	0.355	0.480	0.255	0.590	0.797	0.392	0.550	0.455	0.546	0.447	0.444
FC5	0.519	0.566	0.515	0.494	0.854	0.526	0.553	0.594	0.628	0.502	0.575
INT1	0.471	0.522	0.394	0.471	0.458	0.798	0.356	0.509	0.540	0.502	0.520
INT2	0.346	0.415	0.255	0.506	0.417	0.852	0.362	0.529	0.456	0.498	0.427
INT3	0.372	0.437	0.208	0.360	0.483	0.752	0.310	0.491	0.472	0.347	0.508
INT4	0.312	0.450	0.217	0.454	0.415	0.803	0.379	0.451	0.510	0.393	0.632
PE1	0.582	0.444	0.364	0.340	0.550	0.433	0.824	0.505	0.483	0.281	0.452
PE2	0.352	0.373	0.257	0.426	0.551	0.381	0.769	0.428	0.374	0.388	0.357
PE3	0.445	0.393	0.219	0.380	0.536	0.226	0.785	0.352	0.323	0.334	0.282
PE4	0.307	0.401	0.155	0.427	0.522	0.348	0.792	0.368	0.398	0.464	0.325
RESI1	0.434	0.505	0.453	0.436	0.502	0.433	0.459	0.811	0.568	0.424	0.521
RESI2	0.444	0.515	0.333	0.558	0.520	0.554	0.503	0.810	0.590	0.529	0.526
RESI3	0.427	0.567	0.435	0.378	0.461	0.521	0.327	0.821	0.609	0.352	0.601
SAFE1	0.502	0.587	0.510	0.492	0.539	0.497	0.460	0.658	0.888	0.402	0.631
SAFE2	0.327	0.478	0.319	0.459	0.472	0.423	0.259	0.620	0.810	0.470	0.573
SAFE3	0.449	0.532	0.423	0.460	0.565	0.529	0.482	0.618	0.837	0.383	0.677
SAFE5	0.371	0.518	0.278	0.503	0.523	0.597	0.433	0.489	0.756	0.406	0.628
SI1	0.353	0.389	0.238	0.485	0.385	0.367	0.417	0.445	0.374	0.789	0.353
SI2	0.326	0.464	0.334	0.625	0.491	0.506	0.382	0.403	0.450	0.862	0.505
SI3	0.287	0.490	0.286	0.638	0.513	0.502	0.377	0.502	0.444	0.887	0.525

Note: 1 = availability of cybersecurity, 2 = behavioral intention of adopting cybersecurity, 3 = confidentiality of cybersecurity, 4 = effort expectancy, 5 = facilitating conditions, 6 = integrity of cybersecurity, 7 = performance expectancy, 8 = resilience of cybersecurity, 9 = safety of cybersecurity, 10 = social influence, 11 = use behavior of adopting cybersecurity.

References

1. Hollands, R.G. Critical interventions into the corporate smart city. *Camb. J. Reg. Econ. Soc.* **2015**, *8*, 61–77. [CrossRef]
2. Albino, V.; Berardi, U.; Dangelico, R.M. Smart cities: Definitions, dimensions, performance, and initiatives. *J. Urban Technol.* **2015**, *22*, 3–21. [CrossRef]
3. Kitchin, R. Making sense of smart cities: Addressing present shortcomings. *Camb. J. Reg. Econ. Soc.* **2015**, *8*, 131–136. [CrossRef]
4. Abou-Korin, A.A.; Al-Shihri, F.S. Rapid urbanization and sustainability in Saudi Arabia: The case of Dammam metropolitan area. *J. Sustain. Dev.* **2015**, *8*, 52. [CrossRef]
5. Lacinák, M.; Ristvej, J. Smart city, safety and security. *Procedia Eng.* **2017**, *192*, 522–527. [CrossRef]
6. Alharbe, M.A. Cyber Security, Forensics, and Its Impact on Future Challenges in Saudi Arabia Smart Cities. *Int. J. Adv. Trends Comput. Sci. Eng.* **2020**, *9*, 2464–2470. [CrossRef]
7. Mohammad, R.M.A.; Abdulqader, M.M. Exploring cyber security measures in smart cities. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; IEEE: New York, NY, USA, 2020; pp. 1–7.
8. Townsend, A.M. *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*; WW Norton & Company: New York, NY, USA, 2013.

9. Chen, Q.; Mislove, A.; Wilson, C. Peeking beneath the hood of Uber. In Proceedings of the 2015 ACM Conference on Internet Measurement Conference, Tokyo, Japan, 28–30 October 2015; pp. 495–508.
10. Alkhater, N.; Wills, G.; Walters, R. Factors influencing an organisation's intention to adopt cloud computing in Saudi Arabia. *Int. J. Cloud Comput.* **2018**, *7*, 248–282.
11. Alghazzawi, D.M. A framework to implement cloud computing in e-government in Saudi Arabia. *Int. J. Comput. Sci. Issues* **2012**, *9*, 64–74.
12. Hosam, O.; Ahmad, M.H. Hybrid design for cloud data security using combination of AES, ECC and LSB steganography. *Int. J. Comput. Sci. Eng.* **2019**, *19*, 153–161. [CrossRef]
13. Alshehri, M.; Drew, S.; AlGhamdi, R. Analysis of citizens acceptance for e-government services: Applying the UTAUT model. *arXiv* **2013**, arXiv:1304.3157.
14. Hossam-Eldin, A.A.; Negm, E.; Elgamal, M.S.; AboRas, K.M. Operation of grid-connected DFIG using SPWM-and THIPWM-based diode-clamped multilevel inverters. *IET Gener. Transm. Distrib.* **2020**, *14*, 1412–1419. [CrossRef]
15. AlOtaibi, S.; Aljohani, N.R.; Hoque, M.R.; Alotaibi, F.S. The satisfaction of Saudi customers toward mobile banking in Saudi Arabia and the United Kingdom. *J. Glob. Inf. Manag.* **2018**, *26*, 85–103. [CrossRef]
16. Alrubaiq, A.; Alharbi, T. Developing a cybersecurity framework for e-government project in the Kingdom of Saudi Arabia. *J. Cybersecur. Priv.* **2021**, *1*, 302–318. [CrossRef]
17. Talib, A.M.; Alomary, F.O.; Alwadi, H.F.; Albusayli, R.R. Ontology-based cyber security policy implementation in Saudi Arabia. *J. Inf. Secur.* **2018**, *9*, 315. [CrossRef]
18. Basahel, A.; Yamin, M. Measuring success of e-government of Saudi Arabia. *Int. J. Inf. Technol.* **2017**, *9*, 287–293. [CrossRef]
19. Bryman, A.; Bell, E. *Business Research Methods*; Oxford University Press: New York, NY, USA, 2015.
20. Yilmaz, K. Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *Eur. J. Educ.* **2013**, *48*, 311–325. [CrossRef]
21. Weerakkody, V.; Irani, Z.; Lee, H.; Hindi, N.; Osman, I. A review of the factors affecting user satisfaction in electronic government services. *Int. J. Electron. Gov. Res.* **2014**, *10*, 21–56. [CrossRef]
22. Dillman, D.A.; Smyth, J.D.; Christian, L.M. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
23. Sekaran, U. *Research Methods for Business: A Skill-Building Approach*, 4th ed.; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2003.
24. Saunders, M.; Lewis, P.; Thornhill, A. *Research Methods for Business Students*; Pearson Education: Upper Saddle River, NJ, USA, 2009.
25. Walliman, N. *Your Research Project. A Step-by-Step Guide for the First-Time Researcher*; Sage Publications: London, UK, 2000.
26. Tabachnick, B.G.; Fidell, L.S. *Experimental Designs Using ANOVA*; Thomson/Brooks/Cole: Belmont, CA, USA, 2007; Volume 724.
27. Popova, Y.; Zagulova, D. UTAUT Model for Smart City Concept Implementation: Use of Web Applications by Residents for Everyday Operations. *Informatics* **2022**, *9*, 27. [CrossRef]
28. Kuberkar, S.; Singhal, T.K. Factors influencing adoption intention of AI powered chatbot for public transport services within a smart city. *Int. J. Emerg. Technol. Learn.* **2020**, *11*, 948–958.
29. Van Zoonen, L. Privacy concerns in smart cities. *Gov. Inf. Q.* **2016**, *33*, 472–480. [CrossRef]
30. Mijwil, M.; Doshi, R.; Hiran, K.K.; Al-Mistarehi, A.H.; Gök, M. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects. *Mesop. J. Cybersecur.* **2022**, *2022*, 1–4.
31. Alzahrani, L. Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes. *Int. J. of Adv. Comput. Sci. and Appl.* **2021**, *12*, 630–637. [CrossRef]
32. Alhalafi, N.; Veeraraghavan, P. Cybersecurity Policy Framework in Saudi Arabia: Literature Review. *Front. Comput. Sci.* **2021**, *3*, 89. [CrossRef]
33. Alalwan, A.A.; Dwivedi, Y.K.; Rana, N.P. Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust. *Int. J. Inf. Manag.* **2017**, *37*, 99–110. [CrossRef]
34. Venkatesh, V.; Thong, J.Y.; Xu, X. Unified theory of acceptance and use of technology: A synthesis and the road ahead. *J. Assoc. Inf. Syst.* **2016**, *17*, 328–376. [CrossRef]
35. Arpaci, I.; Sevinc, K. Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Inf. Dev.* **2022**, *38*, 218–226. [CrossRef]
36. McDaniel, C., Jr.; Gates, R. *Marketing Research*; Wiley: Hoboken, NJ, USA, 2006.
37. Hair, J.F., Jr.; Sarstedt, M.; Ringle, C.M.; Gudergan, S.P. *Advanced Issues in Partial Least Squares Structural Equation Modeling*; Sage Publications: Thousand Oaks, CA, USA, 2017.
38. Henseler, J.; Hubona, G.; Ray, P.A. Using PLS Path Modeling in New Technology Research: Updated Guidelines. *Ind. Manag. Data Syst.* **2016**, *116*, 2–20. [CrossRef]
39. Hair, J.F., Jr.; Hult, G.T.M.; Ringle, C.M.; Sarstedt, M.; Danks, N.P.; Ray, S. *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R: A Workbook*; Springer Nature: London, UK, 2021; p. 197.
40. Ali, F.; Rasoolimanesh, S.M.; Sarstedt, M.; Ringle, C.M.; Ryu, K. An Assessment of the Use of Partial Least Squares Structural Equation Modeling (PLS-SEM) in Hospitality Research. *Int. J. Contemp. Hosp. Manag.* **2018**, *30*, 514–538. [CrossRef]
41. Hult, G.T.M.; Hair, J.F., Jr.; Proksch, D.; Sarstedt, M.; Pinkwart, A.; Ringle, C.M. Addressing endogeneity in international marketing applications of partial least squares structural equation modeling. *J. Int. Mark.* **2018**, *26*, 1–21. [CrossRef]

42. Shiau, W.-L.; Sarstedt, M.; Hair, J.F. Internet research using partial least squares structural equation modeling (PLS-SEM). *Internet Res.* **2019**, *29*, 398–406. [CrossRef]
43. Richter, N.F.; Hauff, S.; Ringle, C.M.; Gudergan, S.P. The use of partial least squares structural equation modeling and complementary methods in international management research. *Manag. Int. Rev.* **2022**, *62*, 449–470. [CrossRef]
44. Fornell, C.; Larcker, D.F. *Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics*; Sage Publications Sage CA: Los Angeles, CA, USA, 1981.