IBIMA Publishing
Journal of Information Assurance & Cyber security
https://ibimapublishing.com/articles/JIACS/2021/666987/
Vol. 2021 (2021), Article ID 666987, 15 pages, ISSN: 2165-9923
DOI: 10.5171/2021.666987

Research Article

Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review

Mohammed Alqahtani and Robin Braun

University of Technology Sydney, Ultimo, NSW 2007, Sydney, Australia

Correspondence should be adressed to: Mohammed Alqahtani; Mohammed.Alqahtani@student.uts.edu.au

Received date:13 November 2020; Accepted date: 1st February 2021; Published date: 7 May 2021

Academic Editor: Glorin Sebastian

Abstract

Evidence suggests that, regardless of the number of technical controls in place, organizations will still experience security breaches. Organizations spend millions of dollars on their cyber security infrastructure that includes technical and non-technical measures but mostly disregarded the most important asset and vulnerability the human. Therefore, despite their investments, companies are not able to reap the exact benefits from their security investments because of the human/employee's non-compliance with cyber security policies and measures. Cyber Security compliance is the most effective way to prevent cyber security issues and improve cyber resiliency. To effectively comply with cyber security practices and human acceptance of cyber security technologies, it is important to identify, study and analyze the factors that contribute to their compliance and implementation. This study combines and integrates contemporary literature on the factors of UTAUT2 model related to cyber security compliance. The rationale of this study is to fill the gap of assessing the effect of factors of UTAUT2 model on cyber security compliance. Based on this study, it can be tentatively concluded that the factors influencing technology adoption also affect users' behavior towards cyber security compliance as well as the actual cyber security compliance. This study provides a basic level idea to organizations to formulate a fully functional and useful security compliance framework for their organizations based on factors that influence their employees' intentions and behavior towards cyber security. Consequently, the study is an exciting endeavor to prevent significant security weaknesses and reduce the security breaches in the information systems by explaining different factors that strengthen the users' behavior and intentions to comply with the security. This is an ongoing study, and more information will emerge as it progresses. This is also an ongoing investigation, and further results and findings will be published as the investigation progresses.

Keywords: UTAUT2 model, Security adoption, cyber security compliance.

Cite this Article as: Mohammed Alqahtani and Robin Braun (2021), "Reviewing Influence of UTAUT2 Factors on Cyber Security Compliance: A Literature Review", Journal of Information Assurance & Cyber security, Vol. 2021 (2021), Article ID 666987, DOI: 10.5171/2021.666987

Introduction

Nowadays, with the development of technology, organizations need to properly comply with cyber security measures to prevent cyber-attacks and data leakage. Cyber security compliance is essential to enable companies to better utilize cyber security measures and prevent cyber-attacks (Twizeyimana & Anderson, 2019; Koohang, Nowak, Paliszkiewicz & Nord, 2020). As a result, great attention is currently being paid to the compliance of cyber security requirements and measures in the research industry to ensure information security in organizations and e-government agencies (Herath & Rao, 2009; Huang & Madnick, 2020; Karokola et. al, 2012); Vance, Sipenin and Panila (2012); Roach & Roach (2019); Chalet & Ossey-Bryson (2020). Current research puts forward hypotheses for studying the possible link between technology adoption and cyber security compliance. This study is based on previous research, research and literature showing all possible relationships between variables that influence technology adoption.

Compliance with cyber security refers to changes in a person's behavior, conduct, and attitude due to a pre-established framework that may have been developed to view the requirements and risks to gain effective results of information security. According to the literature, compliance is not a reactive response. It must be viewed as a continuous organizational process. This is why investing in cyber security is more important than ever (Haris & Martin, 2019; Shein, 2020). Cyber security and compliance are inextricably linked. Therefore, to successfully establish information security, organizational security procedures must be aligned with their business goals. Existing research on cyber security compliance mainly focuses on technical and behavioral factors, including factors such as the development and implementation of technical frameworks and employees' attitudes and behaviors related to cyber security compliance (Alzahrani, 2020). Most modern research does not mainly include or address the factors of compliance and technology adoption in the organization.

In addition, the failure of cyber security measures has also allowed unauthorized persons to misuse and exploit information systems, thus increasing security gaps (Ronchi & Ronchi, 2019). Organizations need to set up and implement cyber security frameworks to protect the confidentiality and privacy of users and their data. These strategies should focus on technological advancements such as Data Loss Prevention on the emails of employees that help in preventing employees from sending restricted files and information outside the organization , an authentication mechanism that forces employees to use multiple factors, etc. On the other hand, they must also focus on the factors that directly influence employee's behavior, including technology acceptance, adoption, and cyber security compliance (AlKalbani et al., 2015; Karokola et al., 2012).

This study focuses on the UTAUT2 model for technology adoption (Venkatesh, Morris & Devis, 2003; Venkatesh, Thong and Xu 2012). The main focus of UTAUT is on explaining the behavior and intent of users using technology. UTAUT2 is an extension of the UTAUT model (Venkatesh, Thong & Xu, 2012). However, the available literature does not demonstrate that the UTAUT2 model has been studied for the compliance with cyber security as well as the relationship between the UTAUT2 model and the compliance with cyber security regulations. This study will fill this gap.

Rationale & Objective

The authors of this paper hypothesize that technology adoption factors have a significant impact on cyber security compliance. This is an ongoing study, and at a very preliminary stage now. This hypothesis will be validated with surveys and questionnaires, especially in the context of Saudi Arabia in future work. The study will mainly focus on the impact of technology use for compliance compared to the behavioral change for cyber security compliance. With the advancement in technologies, technology is now able to

enforce the compliance with cyber security policies and measures.

This current study is a preliminary study for future research, and its rationale is to study the UTAUT2 model concerning cyber security compliance in Saudi Arabia. The current paper is an addition to the existing literature in the market that can be used in future research to support and cite different findings and literature.

Literature Review

Cyber security Compliance

Compliance is the implementation of cyber security standards and policies, and these policies are then followed by the employees and organizations for adequate information security (Harris & Martin, 2019). Contemporary research indicates that many security issues arise due to the employees' non-compliance with the cyber security measures (Donalds & Osei-Bryson, 2020; Vance et al., 2012). Similarly, compliance with cyber security frameworks ensures the effectiveness of mechanisms along with threat prevention and risk reduction (AlKalbani, Deng & Kam, 2015; Chen, Chen & Wu, 2018; Choi, Lee & Hwang, 2018; D'Arcy & Greene, 2014; Donalds & Osei-Bryson, 2020; Karokola et al., 2012; Li et al., 2019).

For effective cyber security compliance, users are required to understand, take measures in the direction of compliance (Shappie, Dawson & Debb, 2019), and conform to the security measures (Charlette & Osei-Bryson, 2020). Choi et al. (2018) identified the effect of the employee's behavior on cyber security compliance. The study concluded a positive relationship between users' behavior and cyber security compliance, i.e. cyber security compliance influence employees' behavior.

UTAUT2 Model

The Unified Theory of Acceptance and Technology 2 (UTAUT2) model is a relatively new Model that adopts conceptual and pragmatic likenesses in the previous eight models to explain and analyse the technology adoption process (Venkatesh, Thong & Xu, 2012). The primary aim of the UTAUT and UTUAT2 models is to explain users' behavior and intentions for technology adoption. UTAUT has four constructs: performance expectancy, effort expectancy, social influence, and following facilitating conditions (Figure 1). The first three primarily determine the user's behavioral or usage intention, while the last one directly determines the user's behavior. Age, gender, voluntariness and experience were posited as extraneous variables influencing the four fundamental factors corresponding to their usage intention and behavior (Benbasat & Barki, 2007; Venkatesh et al., 2003).

However, UTAUT2 is an extension of the UTAUT model. Venkatesh, Thong and Xu (2012) anticipated UTAUT2 with new constructs; hedonic motivation, price value and habit have been incorporated (Venkatesh, Thong & Xu, 2012). Although UTAUT2 is a relatively new model, many researches are in progress to test its validity, reliability and suitability within diverse contexts (Venkatesh, Thong & Xu, 2012; Huang et al., 2020).

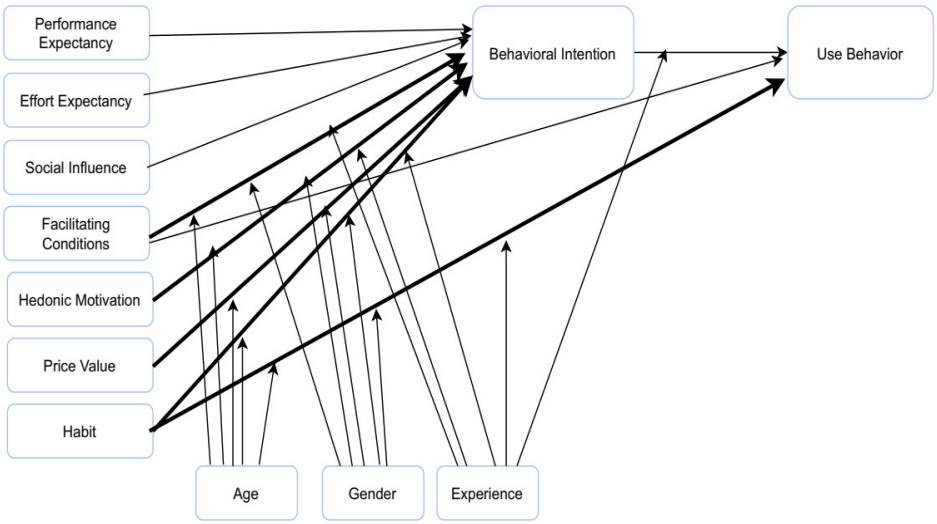

Figure 1: UTAUT2 Model

Technology Adoption overview

Adopting technology refers to making vital decisions regarding accepting, deploying and investing in them (Taherdoost, 2018). Technology adoption can be at the governmental level, organizational level, or individual level. The factors that affect the user's decision of technology utilization should be considered critical at every stage of technology development and deployment (Lai, 2017). On the other hand, the awareness of emerging technologies does not mean that the individual needs to adapt to every novel technology emerging. A company must be equipped with strong decision-making skills to choose a vital technology based on knowledge, experience and acceptance ability.

A number of technology adoption and acceptance models have been developed to determine the relationship between the user's behavior and compliance with technology and its framework (Taherdoost, 2018). These technology adoption models highlight various factors that affect the adoption and behavior of the users. Some of these models may include the Theory of Reasoned Action (TRA), the Theory of Planned Behaviour (TPB), the Technology Acceptance Model (TAM), the Diffusion of Innovation Theory (DIT), the Motivational Model (MM), the Model of PC Utilization (MPU), the Social Cognitive Theory (SCT), the Unified Theory of Acceptance, Use of Technology (UTAUT) and other models (Taherdoost, 2018).

Assessment of UTAUT2 for Cyber Security Compliance through literature

The unified theory of Acceptance and Use of Technology (UTAUT) has been a fundamental model in many studies in order to measure technology adoption and technology use (Maldonado et al., 2011; Fidani & Idrizi, 2012; Ain, Kaur & Waheed, 2015; Gharaibeh & Arshad, 2018). The literature shows that the UTAUT2 model has been used in various researches in various contexts (Table 1).

In the following sections, a relationship of all the constructs with cyber security compliance is stated in detail.

Table 1: Industry-wide Application of UTAUT2

	Contexts	Reference
1	**Mobile Banking Services**	Gharaibeh & Arshad, 2018
2	**Smart Mobile Acceptance**	Ally & Gardiner, 2012
3	**E-Prescribing Technology Acceptance**	Cohen et al., 2013
4	**Broad-Band Internet Adoption**	LaRose et al., 2012
5	**E-Governance Technology**	Krishnaraju et al., 2012; Vinodh & Mathew, 2012

Relationship between technology adoption & cyber security compliance

Cyber security compliance is a multidimensional discipline. These disciplines are interconnected to ensure the implementation of cyber security policies and their compliance across the organization (Charlette & Osei-Bryson, 2020). The development and implementation of technical cyber security measures and the improvement of security strategies are insufficient to protect the critical data stored in an organization; the human factors that influence cyber security must be taken into account with technical controls. The absence of information security awareness; ignorance from the cyber best practices, harms and benefits; carelessness; laziness in following cyber security practices; hatred towards security; and obstruction are the significant causes of users' mistakes (Donalds and Osei-Bryson, 2020). Suppose the end-user and employees of the organization do not consider the importance of these policies and do not practice and follow these policies, in that case, the security of the organization cannot be ensured. Due to this, the individual or personal behaviour aspect of cyber security is essential. Several studies are carried out on the impact of cyber security behavior (Donalds and Osei-Bryson, 2020; Harris and Martin 2019). Many cyber security incidents have been occurred due to the negligence of cyber security policies (Herath and Rao 2009; Harris and Martin 2019; Li et al., 2019).

Cyber security compliance, in a broader sense, is the adoption and acceptance of new technologies. It is hypothesized that cyber security compliance is influenced by technology adoption, which is the primary hypothesis. This is an ongoing research and at a very preliminary stage. The hypothesis will be validated through surveys and questionnaires in later stages, especially in the context of Saudi Arabia. The future study is focused on the impact of technology usage for compliance compared to the behavioral change for cyber security compliance. Technology can be used to enforce the compliance with cyber security policies and measures. However, is this worthy to implement in organizations or organizations should focus on changing their employees' behavior to comply with cyber security policies and measures? This study is a preliminary study for future research. Although this study aims to prove this hypothesis, some literature references are stated here for a preliminary proof of the authors' hypothesis's accuracy. No previous research was explicitly found on this topic, i. e., using technology for cyber security compliance; therefore, the authors are focusing on literature as a preliminary study. In the next stage, it will be validated through surveys and questionnaires.

Performance expectancy

It is the concept of explaining that technology is expected to benefit the users in performing their activities in various ways (Escobar-Rodriguez & Carvajal-Trujjillo, 2014). This construct explains that using technology benefits an individual's

performance at doing his job (Ain, Kaur & Waheed, 2015). Sumak et al. (2010) stated that performance expectancy directly affects behavioral intentions. Engotoit, Kituyi and Moya (2016) investigated the performance expectancy's influence on commercial farmers' intention to use mobile banking communication systems in Uganda. The research interviewed 302 farmers. The findings state that performance expectancy is positively correlated with the commercial farmers' behavioural intentions related to mobile-based technologies of communication in Uganda. This study from Uganda is included because of its relevance to Authentication which is a trait of cyber security.

Similarly, a study was conducted by Marshall et al. (2008) in order to identify the effect of end-users' training on the performance expectancy. The results reported that end-users' training about how to comply with the developed security policies has a positive relationship with the performance expectancy. In another study by (Muller & Lind, 2020), the relationship of PE is also proposed and validated with cyber security compliance.

Effort Expectancy

This construct indicates an individual's belief about the effort or the easiness associated with the technology use (Venkatesh et al., 2003; Escobar-Rodriguez & Carvajal-Trujjillo, 2014). Several studies have been conducted to validate and testify this construct for a relationship with behavior, user intention, and compliance with the security. A result of the study conducted in the context of e-government state that there is a significant positive relationship between the effort expectancy and behavioral intentions of the users regarding e-government technologies (Vinodh & Mathew, 2012). Moreover, (Raman and Don, 2013; Muller & Lind, 2020) also found out that effort expectancy has a significantly positive effect on pre-school teachers' acceptance of learning management systems and security compliance.

Alexandra (2020) conducted a non-experimental correlational research in order to investigate the UTAUT construct's effect on behavioral intentions to comply with the financial services in the National Institute of Standards and Technology Cyber security Framework (NIST CSF), while targeting the participants from professionals of cyber security's financial services. The study's findings analyzed, using multiple regression analysis using SPSS, states that effort expectancy is a significant predictor (with p=0.03 significance level) of behavioral intention for compliance with the National Institute of Standards and Technology Cyber security Framework (NIST CSF).

Social Influence

This factor is associated with the perceived value of the particular technology by the significant others, including friends, family and other influencers (Venkatesh et al., 2003; Escobar-Rodriguez & Carvajal-Trujjillo, 2014, Ain, Kaur & Waheed, 2015). (Yazdanmehr et al. 2020; Alexandra, 2020) undertook a study to determine the moderating role of social influence on information security policy compliance. The study results propel that social influence plays a vital role in weakening and strengthening an individual's compliance towards security policies.

Moreover, Kim and Kim (2017) tried to identify information security usage as compliance management. The data was collected from 975 participants of various Korean energy companies that deployed a compliance system. The study's findings postulated that social pressure is the most significant moderating factor for the participants' compliance behavior, which strongly affected information security adoption and utilization levels. Also, Al-Shafi et al. (2009) reported that peers' beliefs influence employees' views regarding e-government services. Moreover, social influence affects the employees' intention and behavior to use the services of e-government. The Saudi government is aware of e-government benefits. It can get substantial advantages from the e-government implementation for cross

institutions services and delivery of services to citizens and more (Santa, MacDonald & Ferrer, 2019). However, the efforts for implementing e-government in Saudi Arabia have not been carried out completely yet , and the advantage is not yet taken entirely and still in the implementation stage (Al-Zahrani 2020; Santa, MacDonald & Ferrer 2019).

The organizational environment includes colleagues' behaviour, cues for action, and the employee's experience with several other factors (Li et al., 2019). (Herath and Rao 2009; Li et al. 2019) note that employees' behaviour is influenced by their colleagues' behaviour in cyber security, as internal or external motivators. In the organizational cyber security context, people usually tend to behave as their co-workers and friends (Herath and Rao 2009; Venkatesh et al. 2003). (Li et al., 2019) proposed that cues to action are an antecedent to cyber security behaviour. Cyber security behaviour directly leads to cyber security compliance, and 'use behaviour' is a significant construct of the UTAUT2 model.

Similarly, (Avina et al., 2017; Vance et al., 2012) also state a direct relationship between social norms and cyber security compliance behaviour.

Facilitating Conditions

Facilitating conditions refer to the perceived resources and facilities for an individual to perform a particular behavior (Escobar-Rodriguez & Carvajal-Trujjillo, 2014). This aspect also involves the support of an individual from various resources (Venkatesh et al., 2003). Studies show that unavailability or lack of proper resources can hinder students' performance on a web-based technology, and the compliance with security protocols by an organization's employees (Nanayakkara, 2007). Catherine, Geofrey, Moya and Aballo (2017) researched the moderating effect of the UTAUT model's constructs with ATM users' behavioral intentions with fingerprint authentication at banks in Uganda. This was a cross-sectional field study wherein the data was collected from 211 participants of Uganda's ATM users for this quantitative kind of study. The data were analysed using correlation and regression analysis. The results reported that facilitating conditions are strong predictors of behavioral intentions to comply with Uganda banks' fingerprint authentication policies.

Hedonic Motivation

Hedonic motivation is explained as an intrinsic pleasure drive while adapting to technology (Venkatesh et al., 2003; Escobar-Rodriguez & Carvajal-Trujjillo, 2014). A number of researches have reported that hedonic motivation is also known as intrinsic motivation, directly impacting the technology adoption by employees or individuals (Thong et al., 2006; Van der Heijden, 2004). Moreover, Brown and Venkatesh (2005) also found out that hedonic motivation is a significant predictor of technology use and behavioral intention for compliance with security policies. Additionally, Yoo, Sanders and Cerveny (2018) proposed a study to determine the influence of flow (which is a synonym of hedonic motivation) and psychological ownership on security education, training, awareness, and compliance intention of the participants. To conduct this study, a survey methodology was chosen for data collection and the theoretical framework. The study results identified that intrinsic motivation or flow positively influences the employees' security compliance intention.

In their study, (Cialdini and Goldstein, 2004; Griskevicius and Cialdini, 2010) stated that social influence affects behaviour through another person's actions, and the compliance to the cyber security policies is affected by behaviour. The strong influence depends on the ability to induce compliance. Six psychological principles influence the behaviour, and compliance is based upon them. These principles are Consistency, Reciprocity, Liking, Social validation, Authority, and Scarcity. The reciprocity principle states that people are most obliged to pay back the same behaviour, favour, or service they have first received from others. The consistency rule for compliance is that people are consistent with things that they have said previously. A person who

committed something before will be more willing for compliance to request which he/she has committed to a position.

The person may first ask for a small favor, which can be easily complied with. A large favour is then asked, which is generally complied with by those who have previously served the small request. The social validation rule for compliance is that people comply more with a request for the behaviour if other people are doing similar things and consistent with it. The authority rule for compliance states that people tend to comply with the suggestions of persons who have more legitimate authority. Authority may refer to a specific situation or it may denote general authority. The liking principle for compliance is that people generally comply with the request of those individuals whom they most like. Before asking for any favour or request, the target is engaged to liking them. The liking can be increased by physical attractiveness, similarities, compliments, and cooperation. The scarcity rule for compliance is that one tries to get and secure the scarce opportunities. There are varieties of techniques that can convert the power of scarcity to compliance.

As a whole, the above principles cover social, organizational, cultural factors that influence cyber security compliance. When a person requests, explicitly or implicitly, another person, and the individual changes his conduct and behaviour due to this request, this norm is considered compliance. Compliance is a functioning form of social impact because it is ordinarily caused by an individual intentionally. The changes in the internal beliefs and feelings of people sometimes become the reason for compliance. These purposes and changes are primarily not for compliance or they are not necessary to comply, but the compliance may happen because of changes in internal beliefs (Cialdini and Goldstein, 2004; Leandre R. Fabrigar and Meghan E. Norris, 2012).

Price Value

This factor is directed towards the users' perception of the benefits of the application versus the monetary cost of its usage (Escobar-Rodriguez & Carvajal-Trujjillo, 2014). In simple words, it means that the user's positive perception regarding the benefits of technology primarily impacts the user's intention to bear the cost of a particular technology. This is a cost-benefit analysis by the user, which subsequently affects the user's usage intention regarding a technology (Venkatesh, 2012). Ramamurthy and Wen (2014) identified that reward is a beneficial technique to promote employees' compliance behavior. They argued that deterrence or penalties are sometimes ineffective in preventing the non-compliance behavior of the employees. However, rewards have a substantial effect in the direction of the employees' positive intentions regarding compliance with security policies.

Habit

This construct relates to technology's automatic usage because of the habit (Venkatesh et al., 2003). It can also be conceptualised as the performance of an act based on an individual's prior experience. This is because, after the extended use of technology, it becomes a habit that may be referred to as a well-learned action sequence that is stimulated based on some environmental cues and may be repeated involuntarily (Bandyopadhyay & Fraccastoro, 2007). Several prior studies have cited habit as an influential predictor of behavioral intention towards technology usage (Lim et al., 2007; Kim & Kim, 2017; Venkatesh et al., 2012).

Karlzen and Hallberg (2017) studied the relationship between the theory of planned behavior and information security compliance. The hypothesis was tested using 645 white-collar workers; the data were recruited using random sampling, and analysed using correlation and regression analysis. The research results suggested that habit was one of the strongest predictors of information security policy compliance with a correlation of 0.28.

According to (Avina et al., 2017; Herath and Rao, 2009; Vance et al., 2012), social norms

and habits directly influence security compliance behaviour.

Behavioral Intention

Niehoff et al., in their study of the role of organizational behaviour in information system success, found that organizational citizenship behaviour (OCB) ultimately leads to the effectiveness of ISS and OCB, which can improve the individual and organizational compliance with information security policies and lead to success in information systems operations (Yen et al., 2008). Similarly, gender, age, education, and years of work are essential for compliance with security policy (D'Arcy and Herath, 2011; Herath and Rao, 2009).

Another primary reference to this relationship between cyber security compliance and technology adoption is a report published by Sandia National Laboratories (Avina et al., 2017). In this report, the authors stated that security behaviours are adopted based on the user's values and conduct standards. Intrinsic motivation and work rewards are critical for motivating behaviour change. Messaging, communication, and incentives should be tailored to the individual style, values, and attitudes towards cyber security. The individual-level mostly requires behaviour change and resources to implement cyber technology compliance. Avina et al. emphasized the frequency of communication of perceived risks and rewards for cyber technology adoption. Tangible and intangible incentives play an imperative role in an individual's behaviour change for cyber security compliance. They have proved a direct relationship between security behaviour adoptions and personal values and communicating perceived risks. Moreover, in this study, most of the constructs are related to personal behaviour, and perceived risks are a significant construct of the authors' proposed model (Avina et al., 2017). Similarly, security behaviour is the same as behaviour intention of the UTAUT2 model.

A study by (Choi et al., 2018) concluded that employees' behaviour directly relates to an effective ISS compliance. The institutionalization of cyber security policies in practice encourages employees to adopt policies that make their behaviour more compliant. Austin et al. concluded that relevance to the perceived value and legitimacy is defined as internal incentives to comply with information system security (ISS) requirements, positively affecting them.

(Sohrabi Safa et al., 2016) state that sharing information, security knowledge, collaboration, intervention, and expertise significantly affect employees' attitudes towards compliance with organizational information security policies. Additionally, the results showed that personal commitment and norms influence employees' attitudes. Also, the attitude towards compliance with information security policies of an organization strongly influences the behavioural intentions associated with compliance of information security requirements.

The above statements are enough to establish a preliminary relationship between cyber security compliance and technology adoption, and to start a detailed study to analyse each aspect and construct compliance and adoption. This study focuses on proving this relationship and then developing a compliance-based framework for cyber security compliance.

In response to the studies mentioned above and literature, it is found that behavioral intention, social influence, performance, and effort expectancy have a significant influence on the adoption and acceptance of technology and compliance with cyber security in various contexts (see table 2.).

Table 2 : UTAUT2 Relationship with Cyber Security Compliance

UTAUT2 Construct	Relationship with Cyber Security Compliance	Reference
Performance Expectancy	Yes	Ain, Kaur & Waheed, 2015; Sumak et al., 2010; Engotoit, Kituyi & Moya, 2016; Marshall, Mills & Olsen, 2008; El-Gayar & Moran, 2006; Muller & Lind, 2020
Effort Expectancy	Yes	Vinodh & Mathew, 2012; Raman and Don, 2013; Alexandra, 2020;
Social Influence	Yes	Yazdanmehr, Wang & Yang, 2020; Kim & Kim, 2017; Al-shafi, et al., 2009; Alexandra, 2020; Muller & Lind, 2020
Facilitating Conditions	Yes	Nanayakkara, 2007; Catherine, Geofrey, Moya & Aballo, 2017
Hedonic Motivation	Yes	Brown & Venkatesh, 2005; Yoo, Sanders & Cerveny, 2018; Cialdini and Goldstein 2004; Griskevicius and Cialdini, 2010
Price Value	Yes	Ramamurthy & Wen, 2014; Muller & Lind, 2020
Habit	Yes	Kim, et al., 2005**;** Kim & Kim, 2017; Lim et al., 2007; Karlzen & Hallberg, 2017; Venkatesh et al., 2012.
Behavioral Intention	Yes	Sohrabi Safa et al. 2016; D'Arcy and Herath, 2011; Herath and Rao, 2009; Avina et al., 2017; Choi et al., 2018

Theoretical and Practical Contribution

The current study is a useful contribution to the literature as a theoretical and practical framework. Theoretically, this study demonstrates a very new kind of relationship between technology adoption and cyber security compliance, which will contribute to the development of compliance or security frameworks of an organization of public or private sectors or e-governments, not only of Saudi Arabia but across the globe. The study's findings state that the factors that influence technology adoption have a similar effect on cyber security compliance. However, this paper is practically very beneficial for people in authority or administration to plan various factors for their organizations to make their employees more compliant with their deployed frameworks. Hence, this paper will help organizations strategize the security compliance framework that will work effectively.

Limitations & Recommendations

The study's first and foremost limitation is that less data has been cited from Saudi Arabia because of the lack of research on

this topic within the intended context. Special surveys for UTAUT2 constructs and some proposed new constructs that affect cyber security compliance are designed and the authors are working on them. Less data has been cited related to the habit and price value because researchers have ignored these constructs while conducting research. Another limitation can be the vast spectrum of this study; the study has not been done citing the literature from a specific culture or context. However, the study needs to give attention to a specific culture or context, which will further give a detailed look to the factors affecting technology adoption and security compliance in a particular information security cultural setting, which is another important factor to be considered for better understanding (Karlsson et al., 2016).

In the literature review, different literature from other cultures like Uganda, Korea are cited. These are for literature review purposes. The future work in this domain by the researchers will be focused on Saudi Arabia but not on employees from a specific organization. In addition to these limitations, further researches can adopt different adoptions or cyber security models to compare and contrast the results.

Conclusion and Future Work

Cyber security has been one of the most critical factors affecting the efficacious deployment of a security framework. Simultaneously, technology adoption and factors affecting technology acceptance and security compliance are of even more significance. Researchers have reported that many security breaches have been observed because of their non-compliance and negligent behavior. Hence, the current study has described various factors that may be proved effective to lure the employees into complying with a particular organization's security policies. This study has explained the technology adoption utilising the UTAUT2 model and its influence on the employees' compliance intention and behavior. The study's findings identify all of the seven constructs that affect the employee or user's intention and behavior differently towards complying with cyber security. Therefore, the study has established a connection between technology adoption constructs and cyber security compliance.

This is an ongoing research and at a very preliminary stage. The hypothesis will be validated with surveys and questionnaires, especially in the context of Saudi Arabia. The future study will focus on the impact of technology use for compliance compared to behavioral change for cyber security compliance. Technology can be used to enforce compliance with cyber security policies and measures. However, is this worthy to implement in organizations or organizations should focus on changing their employees' behavior to comply with cyber security policies and measures? This question will be answered in the authors' upcoming publications.

References

- Ain, N., Kaur, K. and Waheed, M. (2016). The influence of learning value on learning management system use. Information Development, 32(5), pp.1306–1321.
- AL-Zahrani, M. (2020). Integrating IS success model with cybersecurity factors for e-government implementation in the Kingdom of Saudi Arabia. International Journal of Electrical and Computer Engineering (IJECE), 10(5), p.4937.
- AlKalbani, A., Deng, H. and Kam, B. (2015). Organisational Security Culture and Information Security Compliance for E-Government Development: The Moderating Effect of Social Pressure. In: PACIS 2015 Proceedings. [online] Available at: https://aisel.aisnet.org/pacis2015/65/.
- Ally, M. and Gardiner, M. (n.d.). The moderating influence of device characteristics and usage on user acceptance of smart mobile devices. In: 23rd Australasian Conference on Information Systems (ACIS 2012).
- Bandyopadhyay, K. and Fraccastoro, K.A. (2007). The Effect of Culture on

User Acceptance of Information Technology. Communications of the Association for Information Systems, 19.

- Benbasat, I. and Barki, H. (2007). Quo vadis TAM? Journal of the Association for Information Systems, [online] 8(4), p.7. Available at: https://aisel.aisnet.org/jais/vol8/iss4/7/ [Accessed 2 Feb. 2021].
- Brown and Venkatesh (2005). Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle. MIS Quarterly, 29(3), p.399.
- Catherine, N., Geofrey, K.M., Moya, A.P.M. and Aballo, G. (2018). Effort Expectancy, Performance Expectancy, Social Influence and Facilitating Conditions as Predictors of Behavioural Intentions to Use ATMs with Fingerprint Authentication in Ugandan Banks. [online] undefined. Available at: https://www.semanticscholar.org/paper/Effort-Expectancy%2C-Performance-Expectancy%2C-Social-Catherine-Geofrey/b845c2e6ad39bb07628f470d5a91e30d2343c404 [Accessed 2 Feb. 2021].
- Chen, X., Chen, L. and Wu, D. (2016). Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation-Capability Perspective. Journal of Computer Information Systems, 58(4), pp.312–324.
- Chen, Y., Ramamurthy, K. and Wen, K.-W. (2012). Organizations' Information Security Policy Compliance: Stick or Carrot Approach? Journal of Management Information Systems, 29(3), pp.157–188.
- Choi, M., Lee, J. and Hwang, K. (2018). Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism. Sustainability, 10(5), p.1555.
- Cialdini, R.B. and Goldstein, N.J. (2004). Social Influence: Compliance and Conformity. Annual Review of Psychology, 55(1), pp.591–621.
- Cohen, J., Bancilhon, J.-M. and Jones, M. (2013). South African physicians' acceptance of e-prescribing technology: an empirical test of a modified UTAUT model. South African Computer Journal, 50(1).
- D'Arcy, J. and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. Information Management & Computer Security, 22(5), pp.474–489.
- Donalds, C. and Osei-Bryson, K.-M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. International Journal of Information Management, 51, p.102056.
- Emmanuel Aviña, G., Gordon, S. and Kittinger, R. (2017). Tailoring of cyber security technology adoption practices for operational adoption in complex organizations. [online] Sandia National Laboratories. Available at: https://www.osti.gov/servlets/purl/1596209/.
- Engotoit, B., Kituyi, G.M. and Moya, M.B. (2016). Influence of performance expectancy on commercial farmers' intention to use mobile-based communication technologies for agricultural market information dissemination in Uganda. Journal of Systems and Information Technology, 18(4), pp.346–363.
- Escobar-Rodríguez, T. and Carvajal-Trujillo, E. (2014). Online purchasing tickets for low cost carriers: An application of the unified theory of acceptance and use of technology (UTAUT) model. Tourism Management, 43, pp.70–88.
- Fabrigar, L.R. and Norris, M.E. (2012). Conformity, Compliance, and Obedience. Oxford Bibliographies Online Datasets.
- Fidani, A. and Idrizi, F. (2012). Investigating Students' Acceptance of a Learning Management System in University Education: A Structural

Equation Modeling Approach. [online] . Available at: https://proceedings.ictinnovations.org/attachment/paper/78/investigating-students-acceptance-of-a-learning-management-system-in-university-education-a-structural-equation-modeling-approach.pdf.

- Gharaibeh, M.K., Arshad, M.R. and Gharaibeh, N.K. (2018). Using the UTAUT2 Model to Determine Factors Affecting Adoption of Mobile Banking Services: A Qualitative Approach. International Journal of Interactive Mobile Technologies (iJIM), 12(4), p.123.
- Griskevicius, V. and Cialdini, R.B. (2010). Social Influence. Wiley International Encyclopedia of Marketing.
- Harris, M.A. and Martin, R. (2019). Promoting Cybersecurity Compliance. Cybersecurity Education for Awareness and Compliance, pp.54–71.
- Hassan, L.M., Shiu, E. and Parry, S. (2015). Addressing the cross-country applicability of the theory of planned behaviour (TPB): A structured review of multi-country TPB studies. Journal of Consumer Behaviour, 15(1), pp.72–86.
- Herath, T. and Rao, H.R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), pp.106–125.
- Huang, K. and Madnick, S.E. (2019). Does High Cybersecurity Capability Lead to Openness in Digital Trade? The Mediation Effect of E-Government Maturity within Cross-border Digital Innovation. SSRN Electronic Journal.
- Johnston and Warkentin (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), p.549.
- Karokola, G., Yngström, L. and Kowalski, S. (2012). Secure e-Government Services. International Journal of Electronic Government Research, 8(1), pp.1–25.
- Kim, S.S. and Kim, Y.J. (2017). The effect of compliance knowledge and compliance support systems on information security compliance behavior. Journal of Knowledge Management, 21(4), pp.986–1010.
- Koohang, A., Nowak, A., Paliszkiewicz, J. and Nord, J.H. (2019). Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness. Journal of Computer Information Systems, 60(1), pp.1–8.
- Lai, P. (2017). THE LITERATURE REVIEW OF TECHNOLOGY ADOPTION MODELS AND THEORIES FOR THE NOVELTY TECHNOLOGY. Journal of Information Systems and Technology Management, 14(1).
- LaRose, R., DeMaagd, K., Chew, H.E., Tsai, H.S., Steinfield, C., Wildman, S.S. and Bauer, J.M. (2012). Broadband Adoption| Measuring Sustainable Broadband Adoption: An Innovative Approach to Understanding Broadband Adoption and Use. International Journal of Communication, [online] 6(0), p.25. Available at: https://ijoc.org/index.php/ijoc/article/view/1776 [Accessed 2 Feb. 2021].
- Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, [online] 45, pp.13–24. Available at: https://www.sciencedirect.com/science/article/pii/S0268401218302093.
- Marshall, B., Mills, R. and Olsen, D. (2011). The Role Of End-User Training In Technology Acceptance. Review of Business Information Systems (RBIS), 12(2), p.1.
- Muller, S.R. and Lind, M.L. (2020). Factors in Information Assurance Professionals' Intentions to Adhere to Information Security Policies. International Journal of Systems and Software Security and Protection, 11(1), pp.17–32.
- Nanayakkara, C. (2007). A Model of User Acceptance of Learning

Management Systems. The International Journal of Learning: Annual Review, 12(12), pp.223–232.

- Paola Torres Maldonado, U., Feroz Khan, G., Moon, J. and Jeung Rho, J. (2011). E-learning motivation and educational portal acceptance in developing countries. Online Information Review, 35(1), pp.66–85.
- Raman, A. and Don, Y. (2013). Preservice Teachers' Acceptance of Learning Management Software: An Application of the UTAUT2 Model. International Education Studies, [online] 6(7). Available at: https://files.eric.ed.gov/fulltext/EJ1068463.pdf.
- Ronchi, A.M. (2019). e-Government: Background, Today's Implementation and Future Trends. e-Democracy, [online] pp.93–196. Available at: https://link.springer.com/chapter/10.1007%2F978-3-030-01596-1_5.
- Santa, R., MacDonald, J.B. and Ferrer, M. (2019). The role of trust in e-Government effectiveness, operational effectiveness and user satisfaction: Lessons from Saudi Arabia in e-G2B. Government Information Quarterly, 36(1), pp.39–50.
- Shappie, A.T., Dawson, C.A. and Debb, S.M. (2019). Personality as a predictor of cybersecurity behavior. Psychology of Popular Media Culture.
- Shein, E. (2020). The Role Of Cyber Security In Compliance. [online] Cyber Security Hub. Available at: https://www.cshub.com/security-strategy/articles/the-role-of-cyber-security-in-compliance.
- Simonova, A. (2020). An Analysis of Factors Influencing National Institute of Standards and Technology Cybersecurity Framework Adoption in Financial Services: A Correlational Study - ProQuest. [online] search.proquest.com. Available at: https://search.proquest.com/openview/8482434364a539361dbd14f5dd872752/1.
- Sommestad, T., Karlzén, H. and Hallberg, J. (2017). The Theory of Planned Behavior and Information Security Policy Compliance. Journal of Computer Information Systems, 59(4), pp.344–353.
- Sumak, B., Polancic, G. and Hericko, M. (2010). An Empirical Study of Virtual Learning Environment Adoption Using UTAUT. 2010 Second International Conference on Mobile, Hybrid, and On-Line Learning.
- Taherdoost, H. (2018). A review of technology acceptance and adoption models and theories. Procedia Manufacturing, 22, pp.960–967.
- Twizeyimana, J.D. and Andersson, A. (2019). The public value of E-Government – A literature review. Government Information Quarterly, [online] 36(2), pp.167–178. Available at: https://www.sciencedirect.com/science/article/pii/S0740624X1730196X.
- Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3-4), pp.190–198.
- Venkatesh, Thong and Xu (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly, 36(1), p.157.
- Venkatesh, V., Morris, M.G., Davis, G.B. and Davis, F.D. (2003). User Acceptance of Information Technology: Toward a Unified View. MIS Quarterly, [online] 27(3), pp.425–478. Available at: .
- Vinodh, K. and Mathew, S.K. (2012). Web personalization in technology acceptance. [online] IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/6481794 [Accessed 20 Sep. 2020].
- Weerakkody, V., Irani, Z., Lee, H., Osman, I. and Hindi, N. (2013). E-government implementation: A bird's eye view of issues relating to costs, opportunities, benefits and risks. Information Systems Frontiers, [online] 17(4), pp.889–915. Available at:

https://link.springer.com/article/10.1007%2Fs10796-013-9472-3.

- Yazdanmehr, A., Wang, J. and Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. Information Systems Journal.
- Yen, H.R., Li, E.Y. and Niehoff, B.P. (2008). Do organizational citizenship behaviors lead to information system success? Information & Management, 45(6), pp.394–402.
- Yoo, C.W., Sanders, G.L. and Cerveny, R.P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. Decision Support Systems, 108, pp.107–118.
- Zhang, H., Tang, Z. and Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. Telecommunications Policy, 42(5), pp.409–420.