Examining the Impact of Technical Controls, Accountability and Monitoring towards Cyber Security Compliance in E-government Organizations

Mohammed Alqahtani
Faculty of Engineering and Information Technology
University of Technology Sydney
Ultimo, NSW 2007, Sydney, Australia
Email: Mohammed.Alqahtani@student.uts.edu.au

Robin Braun
Faculty of Engineering and Information Technology
University of Technology Sydney
Ultimo, NSW 2007, Sydney, Australia
Email: Robin.Braun@uts.edu.au
Abstract

IT infrastructure and systems are made up of technical as well as social systems that work in alliance to ensure that organization's goals and objectives are met. Security controls and measures are developed and used to guard data and information systems of the organization. The breaches of Cyber security are primarily caused by the misuse of information systems and failure to comply with cyber security measures. Cyber security non-compliance is a major concern for organizations. For effective compliance and human acceptance of cyber security technology and complying with cyber practices, it is essential to ascertain, research, and examine the factors which contribute to the compliance and implementation of cyber security. This study has utilized an enhanced UTAUT2 i.e. Unified Theory of Acceptance and Use of Technology 2 model and assessed its relationship with cyber security compliance. Five new formal and informal factors that affect cyber security compliance in organizations are identified and evaluated. The research questions addressed are: how the formal factors of technical measures; accountability; monitoring and evaluation impact employee's behaviour towards cyber security compliance. The study comprises a correlational survey of employees working at e-government organizations in Saudi Arabia. Results indicate that there is a significant role play by technical measures; accountability; monitoring and evaluation, on employee attitudes and behaviour towards cyber security compliance.

Keywords: Cyber security compliance, accountability, monitoring and evaluation, technical controls, UTAUT2, compliance relationship

Introduction

The development and proliferation of e-governments and associated services have provided governments with new tools to improve public life, services delivery, engage citizens, and improve work processes (Ronchi and Ronchi 2019; Twizeyimana and Andersson 2019). Such development has also opened up the possibility of data disclosure and unauthorized access to confidential and private data connected to e-government applications. This may obstruct the overall development and implementation of e-governments. Therefore, these issues make cyber security very critical for e-government development and adoption (Alharbi, Papadaki, and Dowland 2017; Huang and Madnick 2020; Karokola, Yngström, and Kowalski 2012; Liu and Carter 2018). According to the studies (Al-Zahrani 2020; Anthopoulos et al. 2016; Franke et al. 2015; Karokola et al. 2012; Liu and Carter 2018; Weerakkody et al. 2015), the critical factors that most researchers highlighted and have significant impact on adoption, acceptance and
implementation of e-governments are security, privacy, and trust. Thus, to build trust and make the public accept and adopt e-government programs and services, governments must adequately address security issues (Al-Zahrani 2020).

One of the major cyber security challenges in organizations is understanding how, together, organizational, personal, and technical factors affect the network security outcome of organizations. Cybercriminals are widely discussed in mainstream media for data breaches and attacks, but there is evidence that most of security breaches are caused by the employees inside the organization whether intentionally or unintentionally due to non-compliance with cyber security measures (Donalds and Osei-Bryson 2020; Kolkowska, Karlsson, and Hedström 2017; Koohang et al. 2020). Indeed, security unaware, incautious and disgruntled employees are more harmful than the external employees because internal employees are always familiar with the critical information of the company and they can easily access the data anytime and any day. (Bulgurcu, Cavusoglu, and Benbasat 2010; Harris and Martin 2019; Li et al. 2019; Shropshire, Warkentin, and Sharma 2015; Siponen, Pahnila, and Mahmood 2014). Most security problems arise from employee non-compliance with cyber security measures (Bulgurcu et al. 2010; Donalds and Osei-Bryson 2020; Vance, Siponen, and Pahnila 2012)

For effective cyber security, compliance with cyber security measures has been taken into great consideration (Herath and Rao 2009; Huang and Madnick 2020; Karokola et al. 2012; Li et al. 2019; S. Raschid Muller and Mary L. Lind 2020; Vance et al. 2012). Generally, when a person changes his or her behaviour, attitude, and conduct due to some explicit request of someone, it is known as compliance (Cialdini and Goldstein 2004; Koohang et al. 2020; Li et al. 2019). Compliance is intentionally prompted by an individual, and it is an active form of social influence (Cialdini and Goldstein 2004; Griskevicius and Cialdini 2010). In cyber security, compliance means effectively implementing and adhering to cyber security policies and standards, and best practices (Harris and Martin 2019; S. Raschid Muller and Mary L. Lind 2020). The implementation and acceptance of standards, and procedures ensure the security of the organization's critical data and information from cyber-attacks, theft, unauthorized access, and fraud (Donalds and Osei-Bryson 2020; Harrell 2014; Harris and Martin 2019; Kolkowska et al. 2017; Koohang et al. 2020). Cyber security compliance confirms the confidentiality, availability, and integrity of data with the government and within the IT infrastructure. Cyber security compliance is increasing in most of the organization to ensure the protection of their valuable data (Harris and Martin 2019; Koohang et al. 2020). Some businesses regard cyber security compliance as a fundamental requirement of their business (Harris and Martin 2019; Hofbauer, Ivkic, and Tauber 2019). Cyber security compliance makes it certain that
cyber security mechanisms will work effectively to prevent threats and reduce risks (D’Arcy and Greene 2014; Donalds and Osei-Bryson 2020; Harris and Martin 2019; Li et al. 2019).

For effective cyber security compliance, users need to understand, take, and conform to the measures taken by the organization to secure its information so that companies can reap the benefits of their technology investments. In (Donalds and Osei-Bryson 2020; Li et al. 2019) the authors concluded that employees’ behavior has a direct relationship with effective information system security compliance. Institutionalization of security policies into practice makes the employees embrace the policies which makes their behavior more complaint (Harris and Martin 2019; Li et al. 2019).

Most of the times, compliance with cyber security requirements not only need change of behavior but also adopting some technology as well. Cyber security compliance, in a broader sense, is the adoption and acceptance of new technologies (AlQahtani and Braun 2020; Avina et al. 2017). For example, deploying a Data Loss Prevention tool for preventing data leak, using token for two factor authentication and many more examples from the technology world. Several critical success factors positively influence technology acceptance and human behavior toward technology adoption. The information technology adoption is the decision of accepting or investing in information technology (Venkatesh, Thong, and Xu 2012). The adoption may lie at the organization level and individual level. User acceptance is vital for the development and improvement of any technology (Barrane, Karuranga, and Poulin 2018; Lai 2017; Venkatesh et al. 2012). The issues that affect users' decision to use technology should be taken into account in any technology development phase. When it is identified that users should accept a particular technology, it will be easy to improve their design and development (Barrane et al. 2018; Lai 2017).

Different technology acceptance models have been proposed and developed in various technological areas to know the users' behavior for adopting technologies (Taherdoost 2018).

The UTAUT (Unified Theory of Acceptance, Use of Technology) model which is a widely accepted technology adoption model (Venkatesh et al. 2003), is a relatively new model that serves as an integrated model. It adopts conceptual and pragmatic similarities in previously adopted models of technology to explain and analyze the technology adoption process (Taherdoost 2018; Venkatesh et al. 2003). UTAUT2 (Venkatesh et al. 2012) is an augmentation of UTAUT (Venkatesh et al. 2003) with some new constructs. The constructs analyzed in these models affect the behavioral intention and usage behavior of that specific technology (Venkatesh et al. 2012).
This study has analyzed UTUAT2 constructs for cyber security compliance. Enough literature is available that link constructs of UTAUT2 model with cyber security compliance. But there are several weaknesses in the previous studies. Most of the previous studies are biased towards a specific group of people and not applicable to general users or employees. For example, the detailed study conducted by (Almaiah, Alamri, and Al-Rahmi 2019; Cuganesan, Steele, and Hart 2018; D’Arcy and Greene 2014; Hu et al. 2012; Liu, Wang, and Liang 2020; S. Raschid Muller and Mary L. Lind 2020; Simonova 2020) are biased in several ways. They have focused on a very limited group of people with specialized professions. For example, in (S. Raschid Muller and Mary L. Lind 2020) Information security personnel have a better understanding regarding information security policies than regular employees (Ahlan, Lubis, and Lubis 2015; Bauer, Bernroider, and Chudzikowski 2017). Previous studies are mostly focused on finding the impact on behavioral intention, not real security compliance behavior. We in this study are focusing on to investigate the actual compliance behavior instead of behavioral intention. Due to the limitations and bias in the previous studies related to technology adoption and security compliance, the results are very weak and difficult to digest. For example, the (S. Raschid Muller and Mary L. Lind 2020) suggested that UTAUT2 may not be a very good model for inspecting Information Security Policy (ISP) compliance amongst information security personnel. It probably not be the case with general public and all employees of the organizations because information assurance professionals usually have more knowledge and bias towards compliance. Therefore, this may not be the case for all employees.

Similarly, the previous studies are focused on some or all of the UTUAT or UTAUT2 constructs, i.e., effort expectance, performance expectancy, hedonic motivations, social influence, facilitating conditions, price value and habit. But there are certain other factors – formal and informal – that are also strong influencers of cyber security compliance. In other words, they force users/employees to comply with certain measures. Formal factors include, technical measures/controls; accountability; monitoring and control; while informal factors include organizational commitment; and end-user awareness. To develop hypothesis to be tested, previous literature on UTAUT2 model with cyber security compliance posits that cyber security compliance can be influenced and impacted by technical measures/controls; accountability; monitoring and control; organizational commitment; and end-user awareness. Data on technical measures/controls; accountability; monitoring and control; and their antecedents are collected through relevant surveys of employees working in Saudi Arabia's e-government organizations. Because in e-government sector, cyber security is paramount and it is often difficult to access its internal cyber
security related data and study it. Results indicate that, technical measures; accountability; monitoring and evaluation play an important role on employee attitudes and behaviour towards cyber security compliance.

The rest of this article is organized as follows: In the next part, we will study existing research on the relationship between constructs of UTAUT2 model and cyber security compliance. Based on a literature review, we presented some research hypotheses and proposed an improved theoretical model of UTAUT2 that took into account new factors important to cyber security compliance. The proposed model shows how these new factors affect employee compliance behavior towards cyber security. These are underlining the description of research design, survey planning and data collection and analysis using statistical means. After that practical and theoretical of the results are discussed, specifically adjusting employee behavior according to cybersecurity requirements is presented. After briefly explaining the limitations of research, conclusion is highlighted, and future research directions are presented.

**Literature Review/ Related Work**

**Relationship between technology adoption & cyber security compliance**

Cyber security compliance is a multidimensional discipline, and these disciplines are interconnected to ensure the implementation of cyber security policies and their compliance across the organization (Donalds and Osei-Bryson 2020; Harris and Martin 2019). For effective cyber security and to ensure the protection of critical data stored with organizations, organizations need to implement and focus on technical aspects of the security as well as the factors that affect the user’s adoption of technology and their behaviour towards compliance. Absence of information security awareness; non-compliance with cyber security policies and requirements; ignorance from the cyber best practices, its harms and benefits; carelessness towards following cyber practices and hygiene; laziness in following cyber security practices; hatred towards security; and obstruction, are the major causes of user mistakes (Avina et al. 2017; Donalds and Osei-Bryson 2020). If the end-user and employees of the organization do not consider the importance of these policies and do not practices and follow these policies, then the organization will be at risk of cyber-attack or a data breach. Due to this, the individual or personal behaviour aspect of cyber security are also essential to be considered in overall cyber security posture. Several studies are carried out on the impact of behaviour on cyber security (Avina et al. 2017; Donalds and Osei-Bryson 2020; Harris and Martin 2019).
Despite a rich literature on technology adoption models and the role of their constructs on user behaviour towards technology adoption, assessing these models for cyber security compliance is lacking. Although some technology adoption constructs have significant impact on individual and organizational cyber security, but still applying these models for cyber security have not engrossed enough attention in information security literature. Some studies are available (Almaiah et al. 2019; Cuganesan et al. 2018; D'Arcy and Greene 2014; Hu et al. 2012; Liu et al. 2020; S. Raschid Muller and Mary L. Lind 2020; Simonova 2020) but their studies are biased towards some specific type of employees, groups, professions and factors.

There are seven key factors that are discussed by UTAUT2 model in order to explain behavioural intentions to adopt and use technology (Venkatesh et al. 2012) – performance expectancy, effort expectancy, social influence, facilitating conditions, hedonic motivation, price value, and habit. Several studies revealed that in the consumer, organizational and individual context, UTAUT2 constructs are strong predictor for cyber security compliance behaviour.

Following is the available literature review of UTAUT2 constructs in relation with cyber security compliance.

**Performance Expectancy**

Performance expectancy refers to the belief that the use of technology in certain situations can be beneficial as it improves performance (Venkatesh et al. 2012). Studies with UTAUT as the theoretical framework have always shown that there is a statistically significant relationship between expected performance and user acceptance of the technology's behavioral intent (Engotoit, Kituyi, and Moya 2016; S. Raschid Muller and Mary L. Lind 2020). (Šumak, Polančič, and Heričko 2010) stated that performance expectancy directly affects behavioural intentions towards use of Moodle, but this study is biased towards students who have already technical skills for using the tool. (Engotoit et al. 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 the usage of mobile-based technologies of communication in Uganda.

Similarly, a study conducted by (Marshall, Mills, and Olsen 2008) in order to identify the effect of end-user 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 (S. Raschid Muller and Mary L. Lind 2020), 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 ease associated with the use of technology (Venkatesh et al. 2012). Several studies have been conducted to validate and testify this construct for a relationship with behaviour, 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 behavioural intentions of the users regarding e-government technologies (Krishnaraju, Mathew, and Sugumaran 2016). Moreover, (S. Raschid Muller and Mary L. Lind 2020) assessed it of information assurance professionals but found non-significant relationship.

(Simonova 2020) conducted a non-experimental correlational research in order to investigate the UTAUT construct’s effect on behavioural intentions to comply with the financial services’ 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 of behavioural intention for compliance with the National Institute of Standards and Technology Cyber security Framework (NIST CSF) (Simonova 2020).

**Social Influence**

This factor is associated with the perceived value of the particular technology by the significant others including friend, family and other influencers (Chang 2012; Venkatesh et al. 2012). (S. Raschid Muller and Mary L. Lind 2020; Simonova 2020; Yazdanmehr, Wang, and Yang 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 behaviour, which strongly affected information security adoption and utilization levels.

The organizational environment includes colleagues' behaviour, cues for action, and the employee's experience with several other factors (Li et al. 2019). According to (Li et al. 2019), they note that their colleagues' behaviour influences employees' behaviour in the field of cyber security as internal or external motivators. In organizational cyber security context, people usually tend to behave as their co-workers and friends (Chen, Chen, and Wu 2018; D’Arcy and Greene 2014; Donalds and Osei-Bryson 2020). In (Li et al. 2019), the author's proposed Cues to action is an antecedent to cyber security behaviour, and cyber security behaviour directly leads to cyber security compliance, and ‘use behaviour’ is a significant construct of UTAUT2 model. Action cues refer to experiences or triggers that can motivate employees to practice cyber security procedures or acquire better security skills. Examples of cues to action include engaging in security awareness programs and social influence. Previous research suggests that peer behaviour is a source of social influence and that social influence is a type of trigger for cues to action that lead to specific experiences. Also, Johnston and Warkentin argue that social influence positively influences people's intentions to take cybersecurity measures (Johnston and Warkentin 2010).

Similarly, (Avina et al. 2017; Cuganesan et al. 2018) also state a direct relationship of social norms with cyber security compliance behaviour.

According to (Cialdini and Goldstein 2004; Griskevicius and Cialdini 2010), social influence affects the 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 professional is based upon. 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, favor, or service they have first received from the others. The consistency rule for compliance is that people are consistent with things that they have said previously. One is 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 complied with easily. A large favor 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 state that people tends to comply the suggestions of persons who have more legitimate authority. Authority may be regarding a specific situation or more it may exercise 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 like them. The liking can be increased by physical attractiveness, similarity, 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 (Cialdini and Goldstein 2004; Griskevicius and Cialdini 2010).

**Facilitating Condition**

Facilitating conditions are referred to as the perceived resources and facilities to an individual to perform a particular behaviour (Chang 2012; Venkatesh et al. 2012). This aspect also involves the support of an individual from various resources (Venkatesh et al. 2012). Studies show that unavailability or lack of proper resources can hinder students' performance on web-based technology and compliance of security protocols by the employees of an organization (Nanayakkara 2007). (Engotoit et al. 2016) researched the moderating effect of UTAUT model's constructs with the ATM users' behavioural 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 analyzed using correlation and regression analysis. The results reported that facilitating conditions are strong predictors of behavioural intentions to comply with the fingerprint authentication policies of Uganda banks.

(Pahnila, Siponen, and Mahmood 2007) proposed a theoretical model in which they found that information quality had a significant effect on actual compliance, threat appraisal and facilitating conditions had a significant effect on attitude toward compliance, and sanctions and rewards did not influence intention to comply or actual compliance.

(S. Raschid Muller and Mary L. Lind 2020) stated that Facilitating conditions are not major factor for compliance for information assurance professionals but could be a significant construct for general public.
**Hedonic Motivation**

Hedonic motivation is explained as an intrinsic pleasure drive while adapting to technology (Chang 2012; Venkatesh et al. 2012). A number of researches has reported that hedonic motivation is also known as intrinsic motivation, directly impacts the technology adoption of the employees or individuals (Venkatesh et al. 2012). Moreover, (Brown and Venkatesh 2005) also find out that hedonic motivation is a significant predictor of technology use and behavioural 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 the 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 has a positive influence on the employees' security compliance intention.

In another study by (S. Raschid Muller and Mary L. Lind 2020), Hedonic Motivation is found to be a strong predictor of behavioural intention and thus have a significant impact on information security policy compliance. Similarly, (Lowry et al. 2013; Silic and Lowry 2020) also devised a non-significant relationship between security and hedonic motivation while working on their Hedonic-Motivation System Adoption Model (HMSAM).

**Price Value**

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

Similarly, (S. Raschid Muller and Mary L. Lind 2020) in their studies concluded that in organizational environment, this construct has no major impact on compliance, but in individual
capacity, this can be a strong predictor. As in organizational environment, the individuals have no concern with the cost implications as they are not paying the cost. On the other hand, cost or price value is a very strong predictor for compliance for organizations due to price of non-compliance or legal or regulatory issues (Haji-Tajuddin 2016; Hofbauer et al. 2019).

**Habit**

This construct relates to technology’s automatic usage because of the habit (Venkatesh et al. 2012). It can also be conceptualized as the performance of an act based on an individual's prior experience. This is because, after 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 and Fraccastoro 2007). Several prior studies have cited habit as an influential predictor of behavioural intention towards technology usage (Kim and Kim 2017; Venkatesh et al. 2012).

(Sommesstad, Karlzén, and Hallberg 2019) studied the relationship between the theory of planned behaviour and information security compliance. The hypothesis was tested using 645 white-collar workers; the data were recruited using random sampling and analyzed using correlation and regression analysis. The research results suggested that habit was one of the strongest predictors of information security policy's compliance.

(Pahnila et al. 2007; Vance et al. 2012) states in their study that habit affect employees’ attitude towards complying with IS security policies.

According to (Avina et al. 2017; Herath and Rao 2009; Vance et al. 2012) Social norms and habit directly influence security compliance behaviour.

In the study performed by (S. Raschid Muller and Mary L. Lind 2020), habit is also a strong predictor of behavioural intention for ISP compliance but only hypothesized for information assurance professionals.

**Behavioural intention**

Niehoff et, al. in their study of the role of organizational behaviour in information system success, they found that organizational citizenship behaviour (OCB) ultimately leads to the effectiveness of ISS and OCB can improve individual and organizational compliance with information security policies which leads to success in information systems operations (Yen, Li,
and Niehoff 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).

Choi et al. (2018) find out in their study of Information Systems Security (ISS) of E-Government for Sustainability, that ISS breaches are becoming the norm rather than the exception, but ISS can only be achieved when employees fully and firmly embrace the concept by changing their behavior to comply with advanced ISS technologies (Choi, Lee, and Hwang 2018). They concluded that employees' behaviour directly relates to effective ISS compliance. The institutionalization of cyber security policies in practice encourages employees to adopt policies that make their behaviour more compliant.

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 requires most behaviour change and resources to implement cyber technology compliance. Avina et al. emphasized the frequency communication of perceived risks and rewards for cyber technology adoption. Tangible and intangible incentives play an imperative role in individual's behaviour change for cyber security compliance. They have proved a direct relationship between security behaviour adoptions and personal values as well as communicating perceived risks. Moreover, in this study, most of the constructs are related to personal behaviour, and perceived risks are a significant construct of our proposed model (Avina et al. 2017).

In (Sohrabi Safa, Von Solms, and Furnell 2016) the authors state that sharing information security knowledge, collaboration, intervention, and expertise significantly affects employee attitudes towards compliance with organizational information security policies. Additionally, the results showed that personal commitment and norms influence employee attitudes. Also attitude towards compliance with information security policies of an organization strongly influences the behavioural intentions associated with compliance with information security requirements.

From the above studies, we have found that technology adoption factors are in one way or the other related to cyber security compliance. Therefore, it can be stated that Cyber security
compliance, in a broader sense, is the adoption and acceptance of new technologies (AlQahtani and Braun 2020; Avina et al. 2017).

It is also pertinent to mention that most of the studies are either biased towards a specific factor, profession, group of people or domain. Similarly, from the literature, we have also devised that there are certain other formal and informal factors that also have significant influence on cyber security compliance. These are technical controls/ measures, accountability and monitoring and evaluation as formal factors, while organizational commitment and end-user awareness are informal factors.

In the next section, we have stated our proposed factors for cyber security compliance and further validated them through surveys and questionnaires.

Table 1 – Summary of Literature Review and Some Weaknesses in the Previous Literature

| S.no | Factor/ Construct | References | Relationship with security compliance or with some trait of security for compliance | Weakness(es) |
|------|-------------------|------------|---------------------------------------------------------------------------------|--------------|
| 1    | Performance Expectancy | (Engotoit et al. 2016; Marshall et al. 2008; S. Raschid Muller and Mary L. Lind 2020; Šumak et al. 2010) | Significant Positive Relationship | Biased towards a specific group of people (Technical students, farmers). Not validated and generalized |
| 2    | Effort Expectancy | (Engotoit et al. 2016; S. Raschid Muller and Mary L. Lind 2020; Simonova 2020) | Significant Positive Relationship by (Engotoit et al. 2016; Simonova 2020) and non-significant relationship by (S. Raschid Muller and Mary L. Lind 2020) | Biased and not generalized |
| 3 | Social Influence | (S. Raschid Muller and Mary L. Lind 2020; Simonova 2020)(Yazdanmehr et al. 2020) (Li et al. 2019)(Cialdini and Goldstein 2004) | Significant Positive relationship by (Simonova 2020; Yazdanmehr et al. 2020) and non-significant relationship by (S. Raschid Muller and Mary L. Lind 2020) (Li et al. 2019) stated a positive influence on compliance (Cialdini and Goldstein 2004) also states a positive influence | (S. Raschid Muller and Mary L. Lind 2020) study is biased towards information assurance professionals. (Simonova 2020) has limitations only application on NIST CSF (Yazdanmehr et al. 2020) study is very detailed but only focuses on SI. (Cialdini and Goldstein 2004) study is focused on general compliance not towards cyber security compliance |
| 4 | Facilitating Conditions | (Engotoit et al. 2016; S. Raschid Muller and Mary L. Lind 2020) (Pahnila et al. 2007) | Significant Positive Relationship by (Engotoit et al. 2016; S. Raschid Muller and Mary L. Lind 2020) | Biased, non-generalized, limited in application |
| 5 | Hedonic Motivation | (Yoo et al. 2018) (S. Raschid Muller and Mary L. Lind 2020) (Lowry et al. 2013) | Significant Positive Relationship by (S. Raschid Muller and Mary L. Lind 2020) and non-significant relationship by (Yoo et al. 2018) | Biased and non-generalized study by (S. Raschid Muller and Mary L. Lind 2020) Domain limited study of (Yoo et al. 2018) |
| 6 | Price Value | (Chen et al. 2012) (Haji-Tajuddin 2016; Hofbauer et al. 2019; S. Raschid Muller and Mary L. Lind 2020) | Unclear Relationship by (Chen et al. 2012) Non-significant relationship by (S. Raschid Muller and Mary L. Lind 2020) | Limited domain-based studies |
| 7 | Habit | (Avina et al. 2017; Herath and Rao 2009; S. Raschid Muller and Mary L. Lind 2020; Vance et al. 2012) | Significant relationship by (Avina et al. 2017; Herath and Rao 2009; S. Raschid Muller and Mary L. Lind 2020; Vance et al. 2012) (Bandyopadhyay and Fraccastoro 2007; Sommestad et al. 2019) | Limited domain-based studies and biased towards certain groups |
| 8 | Behavioural Intention | (Choi et al. 2018; D’Arcy and Herath 2011; Herath and Rao 2009; Sohrabi Safa et al. 2016) | Significant influence on security compliance | Focused on behavioural intention rather than actual compliance behaviour |

**Proposed Model**

In developing the hypothesis to be tested, a detailed study of the prior literature on cyber security compliance, user behaviour towards cyber security compliance, UTAUT2 constructs and its relation to cyber security compliance is carried out. Literature posits that cyber security compliance can also be influenced and impacted by technical measures/controls; accountability; monitoring and control; organizational commitment; and end-user awareness.
In the literature review, several references have been stated to establish a relationship between technology adoption to cyber security compliance. All the major constructs of UTAUT2 model are directly related to cyber security compliance. But there are several weaknesses in the previous studies. Most of the previous studies are biased towards a specific group of people and not generalized. For example, the detailed study conducted by (S. Raschid Muller and Mary L. Lind 2020; Simonova 2020) are biased in several ways. They have focused on a very limited group of people and that group was information assurance professionals (S. Raschid Muller and Mary L. Lind 2020). Information security professionals are expected to have a better understanding of information security policies than regular employees (Ahlan et al. 2015; Bauer et al. 2017).

Previous studies are mostly focused on finding the impact on behavioural intention, not real security compliance behaviour. This study is focused on investigating the actual compliance behaviour instead of behavioural intention.

Due to the limitations and bias in the previous studies related to technology adoption and security compliance, the results are very weak and difficult to digest. For example, the (Muller & Lind, 2020) suggested that UTAUT2 may not be a good model for examining ISP compliance amongst security professionals. This may not be the case with general public and all employees of the organizations because information assurance professionals usually have more knowledge and bias towards compliance. Therefore, this may not be the case for all employees.

Similarly, the previous studies are focused on some or all of the UTUAT or UTAUT2 constructs, but literature also posits some other factors which are also strong influencers of cyber security compliance. In other words, they force users/ employees to comply with certain measures. Formal factors include technical measures/ controls; accountability; monitoring and control; while informal factors include organizational commitment; and end-user awareness.

In this study, we are focusing only on the formal factors. The informal factors will be discussed and validated in another study.

The below figure (Figure 1) is an abstract of our proposed enhanced UTAUT2 model for cyber security compliance.

In the next sections, proposed new factors are discussed in detail and validated for cyber security compliance.
Technical Controls/ Measures

Technical controls (also called logical controls) include hardware or software mechanisms that are deployed to protect organizational assets from cyber breaches. These controls provide automatic protection against unauthorized access and misuse, facilitate detection of security breaches, and support application and data security requirements (Dempsey et al. 2011; Toth et al. 2014; US Department of Commerce 2006). Typical examples are authentication solutions, Data Loss Prevention (DLP) solutions, firewalls, two-factor authentication, anti-malware solutions, intrusion detection and prevention systems (IDPS), constrained interfaces, and access control lists (ACLs), encryption and many more measures.

Technical security measures help in ensuring compliance towards protecting the information systems. In other words, we can state that technical controls are the major way to enforce and provide conditions towards security compliance. These can be explained through some examples.

Let suppose an organization has deployed a Data Loss Prevention (DLP) solution and a policy is enforced technical on the DLP that any document with Secret or Confidential Label will not leave the organization by any means like, not be printable, not being sent through email not copied to any removable media, not able to upload to any internet or cloud storage. Suppose an employee intentionally or unintentionally tries
to send that document to someone outside the organization through email. When the employee selects the
document to attach to email, the DLP solution detect the label and stop the process by warning the
employee that this is against the security policy. In this way the employee willingly or unwillingly
complies with the policy. The above example is a way to comply with a policy like “A prohibition on
transferring sensitive data to another device not in compliance with the policy.”

Another example is, suppose the organization have a policy that the document/ data with Secret label at
rest will be encrypted with AES-256-bit encryption. When the user/ employee creates a file with a secret
label, the underlying security control for encryption will ask a key from the user for encryption. Now
either willingly or not, the user has to supply a key for encryption. Thus, making enforced compliance.

Although these controls are most of the times not accepted willingly by the employees and creates stress
but on the other hand makes the employees to comply with security policy. To investigate and test this
factor further, following hypothesis are formulated:

H1: Automatic Enforcement of Security Controls foster increase intent to comply with cyber security
policy.

H2: Technical Security Controls are more helpful in following of security policies and compliance

**Accountability**

A promising way to change user behavior is through accountability. In other words, accountability is
defined as "using pressure implicitly or explicitly to justify our beliefs and actions in front of others"
(Anon 2010; Breaux et al. 2006; Goodman and Lin 2007; Vance, Lowry, and Eggett 2013). Accountability
building has received considerable attention in psychology and organizational behavior (Lerner and
Tetlock 1999). Previous studies have consistently shown that if a person is expecting that s(he) will be
held responsible and accountable for some action, reduces the likelihood that the person will behave in a
socially unacceptable way (Breaux et al. 2006; Feigenbaum et al. 2011; Goodman and Lin 2007; Sedikides
et al. 2002; Vance et al. 2013). Although people have long recognized the power of information
technology systems (ITs) to control insiders (Goodman and Lin 2007), no research has been conducted on
the psychological impact of information systems (IS) accountability.

Accountability is key to security and compliance (Breaux et al. 2006; CommandHound 2019; Goodman
and Lin 2007; Vance et al. 2013). Some employees ensure that all tasks are completed on time and as
required, while others are not thinking the same with a low success rate, even they know these tasks are
important and can prevent, transfer, or mitigate business risks. Why can't I achieve the same level of success, even if I'm aiming for it? Is that their motive; their DNA; compensation; culture or what? Chris Duggan, CEO of BetterWorks, a Palo Alto-based software company, said in an interview with Monster: "Bonus or promotion may give someone a special interest for a few days, but this won't be achieved until the end of the year, or change their motives." (CommandHound 2019) So if these are not due to rewards, then what is this? Are these area results of different management and organizational behavior frameworks and theories, like: Individual and team KPIs related to business strategy, balanced scorecard, performance assessments, empowerment of employees, etc.

All of the above theories, organizational processes and controls, are good at their capabilities, but they show different results when building a culture of accountability. The link that is lacking is 'accountability' (Vance et al. 2013). If employees are directly responsible for a particular task or follow policies, controls, or procedures, success can be easily measured by whether the task was completed on time and according to the policy. The employee complies with policy or not. By tracking employee progress, you can easily and quantitatively analyze performance. When employee realize that things are measurable and that the rewards, promotions, perceptions and consequences of these aspects, will motivate people to work. **This will significantly improve the compliance, quality and risk mitigation** (CommandHound 2019; Feigenbaum et al. 2011; Sedikides et al. 2002; Vance et al. 2013).

For example, in the previous DLP example, in the absence of the DLP solution, if the employee know that all the actions are being monitored and logs are verified daily and this action may be caught by compliance department or security guys. And as this is totally against policy, I can be terminated by the organization. This though of accountability will deter him to proceed with the task not complying with organizational policy.

To investigate and test this factor further, following hypothesis are formulated:

H3: Increased perceptions of accountability by employees deter security controls and policy violations

H4: Accountability is a significant predictor of compliant behavior among participants.

**Monitoring and Control**

Evaluation is the belief that “according to some basic rules, the performance of an individual will be evaluated and assessed by another individual and has some implied consequences” (Lerner and Tetlock 1999, p. 255). In particular, most of the information used in the assessment and evaluation comes from
the monitoring process, therefore they are complementing each other. Monitoring is the process of observing and tracking a person's actions (manually or automatically) (Boss and Kirsch 2007; Griffith 1993). Therefore, our research has two foundations: (1) the organization tracks and observes (monitoring) a person's behavior (2) The person expects to be judged on the basis of observed or recorded behavior. Research has shown that evaluation awareness improves socially desirable and acceptable behavior (D’Arcy and Greene 2014; Harrell 2014; Hochwarter et al. 2007; Lerner and Tetlock 1999) and prevents the person from performing socially unacceptable behavior (Herath and Rao 2009; Sedikides et al. 2002).

Monitoring and Control or in other words Monitoring and evaluation is another strong predictor of cyber security compliance. This construct is directly related to accountability, because without strong monitoring and evaluation mechanisms, the accountability cannot be enforced. If individual’s perception of accountability is strong and observed by the individual, then the compliance behaviour will be strong.

For example, those who are aware of monitoring and evaluation, know that their work and behavior may be directly or indirectly observed by others, especially in the case of non-compliance and misconduct at work, i.e., by not following the cyber security policy requirements, will try their best to follow the policy. Monitoring and evaluation can be used in the context of cyber security compliance as an effective way to support and facilitate security compliance. When such monitoring and evaluation is part of the regular IT and security management, such monitoring and evaluation is effective and makes insiders expect that they are being monitored for their actions towards compliance. Monitoring, evaluating and performing system audits are also used effectively to ensure compliance with data protection laws. To investigate and test this factor further, following hypothesis are developed based on literature review:

H5: Monitoring and Evaluation that foster identification and accountability will increases socially desirable behaviours towards compliance.

H6: Monitoring and Evaluation decrease intent to commit cyber security policy violations.

**Research Methodology**

The present study utilized (Venkatesh et al. 2012) UTAUT2 model to find the relationship between technology adoption and cyber security compliance. In this specific document, the major UTAUT2 constructs are not directly assessed through survey but only three of the proposed factors, i.e., technical controls/ measures, accountability and monitoring and evaluation are assessed. In this study, we are
focusing on the impact of these factors specifically on compliance. Other affects that are caused by these measures like stress, lack of motivation etc. are not part of this study.

**Research Design**

The research has used quantitative design undertaking survey method. Correlational study design is used in the research to find out the impact of independent variables (i.e., technical control/measures, accountability and monitoring and control) on dependent variables (i.e., compliance). (Salkind 2012) stated that “the correlation research method finds out the relationship between two or more variables.”

**Data Collection and Participants**

A survey method was used to test our proposed model, a single survey was conducted for this study. The survey covers the three formal factors that influence cyber security compliance. Survey Monkey was used to develop the survey and distributed via different channels, i.e., WhatsApp, Emails, Facebook Messenger. All the participants were working professionals from e-government organizations from Saudi Arabia. The questionnaires were distributed among almost 300 applicants, and 182 complete questionnaires were obtained, reflecting a response rate of 61%. So, the total data is taken from 182 participants (male = 131, females = 51) from diverse socioeconomic background. From the participants 72% were male and rest of 28% participants were females. 52.7 % of the participants were aged between 20–39. All of the participants have received at least graduation level education. Additionally, most of the participants (71.1 %) had more than five years of work experience belonged to IT/ Telecom field (64.7%). The participants were enrolled using mixture of purposive random sampling along with snowball sampling wherein, the initial participants were approached using referrals and then they were asked to refer further participants. Furthermore, no inclusion and exclusion criterion were set other than the inclusion of the only participants working in e-government organizations in Saudi Arabia.

**Procedure**

First of all, the permission was taken to conduct this research from the university dean. After that consent form from the participant was also signed besides briefing them about the purpose of research. The participants were assured about the confidentiality of their data. The data was collected using online platform administering a questionnaire which was divided into three sections; research debriefing and consent form, demographic sheet and final questionnaires. The detailed overview of the questionnaire is given in the “Measures” section. These questionnaires were shared with the participants and they were
asked to send back the filled questionnaire as soon as possible. Aside, the participants were also asked to only be part of research if they are willing to be. They were also requested to provide completed questionnaire and sincere responses without any kind of bias. Moreover, the participants were also asked to refer more participants for the research. The participants were administered four types of primary questionnaire along demographic sheet; technical control, accountability, monitoring and control and compliance. The statistical analysis is done using latest version of SPSS (version 24). The final results of the tests are described in detail under Result section along with a thorough discussion over them.

**Ethical Considerations**

The research was exactly done being within the boundaries of National Guideline Regarding Research Ethics in Saudi Arabia mentioned in book Research Ethics in Arab Region by (Silverman 2017). The current research is ethically approved especially because it doesn’t include any human or animal harm. It also doesn’t hurt any emotion or sentiments of Muslims. The permission from corresponding bodies is also taken to make this research ethically approved. Furthermore, the confidentially and privacy of the participant will be never breached. The data provided by the participants will be secured for 5 years and after that it will be discarded.

**Statistical Analysis**

For analysis of the data Statistical Package for Social Sciences version 24 was used. First of all, the data was exported from the questionnaire and entered into the SPSS. The coding for reverse item was redefined. The mean score of each scale was collected by adding up all of the items score and dividing by total number of items of the respective scale. High scores on Technical Measures, Accountability, Monitoring and Control and Compliance scales shows high level of corresponding phenomenon. The data was firstly run for descriptive statistics along with detailed output of outliers. The data met all of the assumptions of running a parametric test along with the normal distribution of data, depicted by absence of abnormal outliers. After that, “Pearson Correlation Coefficient” was employed on the data to find out the correlation. “Multiple Hierarchical Linear Regression” was also applied on the data to further validate the correlation results. The descriptive statistics included mean, standard deviation, frequencies and percentages, skewness and kurtosis of the demographic variables. Reliability analysis of the data was also done which was found satisfactory. The alpha level is set at \( \alpha .05 \) in this study.
Measures

There were three basic sections of questionnaire: research debriefing and consent form, demographic sheet and final questionnaires. The first section briefed about the research’s purpose and required a sign for consent to be participant of the research (See Appendix 1). The second section was referred to the demographics wherein various questions were asked regarding field and history of participant. The third was the main section of the questionnaire which included four questionnaires: technical control, accountability, monitoring and control and compliance. Each of them is described in detail below.

Demographic Sheet

The demographic sheet included 7 questions to inquire about the participant’s age, gender, job position, organization, level of education, size of organization and work experience. This section was important to collect data about the general background of the participant to report about the field and other specific information of the participant so that research can be generalized accordingly (See Appendix 2).

Technical Control/Measure

In the second section the questionnaire was about technical control and measures. The questionnaire consisted of 12 total items having same format of response. It is a 6-point Likert type scale wherein the answer to the question ranged from “Strongly Agree” to “Strongly Disagree”. In SPSS “strongly agree” was codded as “6”, “agree” as “5”, “somehow agree” as “4”, “somehow disagree” as “3”, disagree” as “2” and “strongly disagree” as “1”. For scoring there is not any kind of cut off scores and the technical measures’ score is gauged from mean number, i.e., responses to the items will be summed up and divided with the number of items that is 10, to yield the final score. The questionnaire was in English language because the participants were from educated and belonged to different fields hence it was easy for them to answer the questions in English. High scores on this scale depicts strong implication and compliance with technical measures. Moreover, the items of the questionnaire were inclined to inquire about the participant’s views about technical control and measures and the technical measures implemented in the corresponding companies to whom the participants were affiliated with. Finally, the reliability of this scale is tested using Cronbach’s Alpha score that were 0.78 which means a high reliability (See Appendix 3).

Accountability

The second questionnaire is about accountability of the participants by their corresponding company. This questionnaire consisted of pool of 15 items, having same format of response. The ranging and
markings were same as other factors. The items of the questionnaire were inclined to inquire about the participant’s views about accountability and if comply with the policies out of fear of accountability? So that the impact of accountability’s fear can be gauged on compliance behavior of the participant. Finally, the reliability of this scale is tested using Cronbach’s Alpha score that were 0.67 which means a good reliability (See Appendix 4).

**Monitoring and Control**

The third questionnaire inquires about the monitoring and controlling employed on participant by their company, in order to find out the impact of monitoring and controlling on compliance behavior of the participant. This questionnaire consisted of pool of 10 items, having same format of response. The items of the questionnaire were inclined to inquire about the general view of the participants regarding monitoring and control along with the specific level of monitoring and control administered over them by their company. Finally, the reliability of this scale is tested using Cronbach’s Alpha score that were 0.72 which means a moderate level of internal consistency of the scale (See Appendix 5).

**Compliance**

The fourth and final questionnaire is about Compliance. This will measure the scores of dependent variables. This questionnaire consisted of pool of 10 items, having same format of response. High scores on this scale depicts high level of compliance behavior of the participants with cyber security policies of their company. Finally, the reliability of this scale is tested using Cronbach’s Alpha score that were 0.83 which means a high level of reliability with highest internal consistency related to the other used scales (See Appendix 6).

**Results**

| Variables                  | $K$ | $\alpha$ | $M$   | $SD$ | Skewness | Kurtosis |
|----------------------------|-----|----------|-------|------|----------|----------|
| Technical Measures/Control | 12  | .78      | 39.63 | 4.76 | .03      | -.24     |
| Accountability             | 15  | .67      | 34.1  | 2.76 | .14      | .07      |
| Monitoring of control      | 10  | .72      | 35.01 | 3.38 | .28      | .04      |
Reliability analysis was done to check the reliability of the scales used in the study. The Cronbach alpha reliability of the Technical Measures/Control scale ($\alpha=.78$), Accountability ($\alpha=.67$), Monitoring of control ($\alpha=.72$) and Compliance ($\alpha=.83$) were found satisfactory. The data is approximately normally distributed as all the skewness and kurtosis values lies between the acceptable range of $+2$ and $-2$ (George and Mallery 2019).

Table 3 - Pearson Correlation Coefficient among Technical Measures/Control, Accountability, Monitoring & control and Compliance (N=182)

| Variables | 1   | 2     | 3   | 4   |
|-----------|-----|-------|-----|-----|
| 1. TMC    |     | -.20*** | .001 | .54** |
| 2. AC     |     | --    | .23*** | .71*** |
| 4. MC     |     | --    |     | .33* |
| 5. CO     |     | --    |     |     |
| 6. M      | 39.63 | 34.1  | 35.01 | 43.00 |
| 7. SD     | 4.76 | 2.76  | 3.38 | 14.36 |

Note: N=182; ***p<0.001, **p<0.01, *p<0.05; TMC= Technical Measures/Control, AC= Accountability, MC= Monitoring & control, CO= Compliance Scale., M= mean, SD= Standard Deviation.

The above-mentioned Table 3 is showing the results of Pearson Product Moment Correlation Coefficient determining the relationship between technical control, accountability, monitoring and control and compliance. First of all, the assumptions of Pearson Correlation tests were fulfilled including the continuity of all variables, normality assumption by checking the skewness and kurtosis value which was within the range of $\pm 2$, the assumption of no extreme outliers, independent observations and linear relationship were also met. The results are showing a significant, moderate positive relationship between technical measures/control and compliance ($r=.54$), while accountability and compliance showed highly
significant, strong positive relationship. Moreover, monitoring and control showed significant low positive relationship with compliance. In layman terms, it means that if a company have implemented good technology measures/control, it will be having moderate effect on compliance behavior. While high accountability will be having higher effect on compliance behavior of cybersecurity. Comparatively, the effect of monitoring and control is lower on compliance behavior of the employees.

Table 4 - Multiple Hierarchical Linear Regression showing the predictors of technical control, accountability, monitoring and control and compliance (N=182)

| Predictors                  | ΔR² | B   | SEB  | β       |
|-----------------------------|-----|-----|------|---------|
| Model 1                     | -.01|     |      |         |
| Gender                      |     | -.02| .2   | .07     |
| Model 2                     | .06**|    |      |         |
| Technical Control           |     | .07 | .05  | .54**   |
| Model 3                     | .05***|  |      |         |
| Accountability              |     | .24 | .69  | .71***  |
| Model 4                     | .007*|    |      |         |
| Monitoring and Control      |     | .01 | .4   | .33*    |
| Total                       | 1.207|    |      |         |

Note: N=182, ΔR²=Change R square, β= Beta, SEB= Standard Error Beta ^p<0.001, ^p>0.001, p>0.01

The above Table 4 is showing the results of Multiple Hierarchical Linear Regression determining the predictors of technical control, accountability, monitoring and control and compliance. Multiple Hierarchical linear regression was run to predict technical control based on the predictors of accountability, monitoring and control and compliance. In model 1 gender was entered as a control variable, in mode 2 technical control was added as predictor, in model 3 accountability was added as
predictor and in model 4 monitoring and control was added as predictor. Assumptions for independent errors were tested by the Durbin Watson test and the value (1.76) was within the range of 1-3, showing that the assumption was met. Another assumption for no perfect multicollinearity was assessed by determining the tolerance value and all the values were above .2 thus meeting the criteria.

In the first model for technical control, control variable such as gender was added and significant regression equation was found non-significant, $R^2=0.01, F(1, 182)=1.17, p=1.02$. In model two technical measures/control was added along with the effect of gender the regression equation was found significant $R^2=0.07, F(2, 182)=1.71, p=0.006$. When the effect of model 1 was subtracted from model two the regression equation still found significant $\Delta R^2=0.06, F(1, 182)=0.54, p=0.004$. In model 3 accountability was added along with the effect of gender and technical measures/control were added and the regression equation was found significant $R^2=0.12, F(3, 296)=2.42, p=0.001$. When the effect of model 1 and model 2 was excluded from model 3 the regression equation found still significant $\Delta R^2=0.05, F(1, 296)=0.71, p<0.001$.

Moreover, in Model 4 monitoring and control was added along with effect of gender, technical control and accountability, the regression was found significant with $\Delta R^2=0.165, F(1, 296)=2.42, p<0.01$. When the effect of model 1, model 2 and model 3 was excluded from model 4 the regression equation found still significant $\Delta R^2=0.007, F(1, 296)=0.33, p<0.01$. Among predictors monitoring and control has emerged as significant weak positive predictor ($p=0.01$) respectively. Technical control and measures are significant moderate positive predictors of compliance ($p=0.004$), accountability has emerged as the strongest positive predictor of compliance ($p=0.001$) and monitoring and control are the weak of academic procrastination among university students. Which means that increased level of technical measures, accountability and monitoring and control have impact of compliance and caused high compliant behavior among participants, wherein, gender doesn’t have effect on compliance behavior at all, monitoring and control have slightly less effect, technical measures have moderate effect and accountability have greatest effect on compliant behavior of the participants.

**Discussion**

**Technical Controls/ Measures**

To investigate and validate this factor, following hypotheses were formulated:
H1: Automatic Enforcement of Security Controls foster increase intent to comply with cyber security policy.

H2: Technical Security Controls are more helpful in following of security policies and compliance

Both of the above-mentioned hypotheses are well supported by the result of Pearson Correlation and Multiple Hierarchical linear Regression test’s results. The results of the Pearson Correlation test indicated that there is a significant, moderate positive relationship between technical measures/control and compliance (r=.54), that means the companies who have enforced technical measures are more likely that their employees will be complying with the security policies. At the same time the results of Multiple Hierarchical linear regression also find out that technical measures are significant moderate predictors of compliance, which means technical measures have ability to positively moderate the compliance behaviors of the employees.

The existing literature also support the current findings of the research.

Accountability

The following hypotheses were hypothesized:

H3. Increased perceptions of accountability by employees deter security controls and policy violations

H4. Accountability is a significant predictor of compliant behavior among participants.

The results of Pearson Product Moment Correlation Coefficient (PMCC) and Multiple Hierarchical linear Regression have also supported this hypothesis. Thus, null hypothesis for this has been rejected. The PMCC results have identified that accountability is the most responsible factor that helps the employees comply with the security policies of the corresponding company, by showing significant strong correlations between the two variables, i.e., accountability and compliance. Moreover, result of Multiple Hierarchical Linear Regression also found that accountability is a strong positive predictor of compliance behavior.

In line of the current findings, a number of findings have been cited in the existing literature. For example, (Passyn and Sujan 2006) conducted a study to identify role of self-accountability in behavioral compliance. They found that accountability is the most important factor that induces fear in the individual and acts as a motivator to comply with the said behavior. In another study by (Sanders, Reckers, and Iyer 2008) carried out a research to verify that accountably predicts compliance among tax payers. The results
of their research indicated that tax payers were more likely to comply with the policies if they were more fearful of accountability and penalty. (Hanawalt 2018) studied the teachers to verify the role of accountability in compliance. The results of the study showed a positive relationship between the variables. This meant that when the teachers were more aware of accountability, they were more likely to comply with the policies. Similarly, (Kennedy, Emmanuel, and Izedonmi 2012) inclined to examine the relationship between government accountability and compliance of tax payers. The results of the studies affirmed that an individual’s perception of government accountability plays an instrumental role in the maintenance and compliance behavior of the taxpayers.

Hence the aforementioned literature showed a clear support to the current results, however the strength of the relationship is inconsistent among various studies not directly in the field of Information systems (Hanawalt 2018; Kennedy et al. 2012; Passyn and Sujan 2006; Sanders et al. 2008).

**Monitoring & Control**

The following hypotheses were hypothesized:

*H5. Monitoring and Control are significantly related to compliance.*

*H6. Monitoring and Control predicts the compliant behavior among participants.*

These hypotheses were also supported by the results of PMCC and Multiple Hierarchical Linear Regression. The result of PMCC indicated that monitoring and control has significant relationship with policy compliance among participants. Similarly, Multiple Hierarchical Linear Regression also evidenced that monitoring and control is a weak predictor of compliant behavior among participants, thus rejecting null hypothesis.

The existing literature also have evidenced that monitoring and control has relationship and predicts compliance with policies by the employees. (Balozian and Leidner 2017) carried out research to identify the factors effecting the employee’s behavior of compliance. The researchers found that monitoring and control were one of the factors that strongly effects the compliance behavior of the employees regarding security compliance. The variance of relationship strength between the cited research and the current research may be due to difference of context and geographical location where the research has been complied. Because the cited research is done among participants of western culture, while the current research has been done in the Saudi Arabian cultured companies and employees.
Theoretical and Practical Contributions

This study poses a number of theocratical and practical contributions towards user’s cyber security compliance behaviours in organizations.

In theory, the study contributes to cyber security compliance by identifying new factors that directly impact user behaviours and attitude towards cyber security compliance. The authors identified and established that technical measures, accountability and monitoring and control have a significant impact on cyber security compliance in organizations. This will help organizations and governments to device strategies based on these factors for effective cyber security compliance for preventing security and data breaches.

This research demonstrates practical contribution on how to maintain effective cyber security compliance in public organizations by two ways. First, to identify and establish a strong relationship between the identified factors and cyber security compliance. Second, developing a preliminary framework for effective cyber security compliance based on the factors that affect cyber security compliance. It offers organizations and governments the opportunity to better plan cybersecurity strategies and cybersecurity investments. This can be done by focusing on the important factors that directly affect employee's security compliance and enhance e-government security in public sector organizations. When organizations know the crucial factors that affect cyber security compliance, they can create a supportive environment in which the employees will nurture effective security compliance.

Conclusion and Future Work

The aim of this research was to identify the factors that influence user behaviour towards cyber security compliance. For this purpose, five factors — Technical Controls/ Measures; Accountability; Monitoring & Control; Organizational commitment; and End User Awareness — were identified from literature and assessed for cyber security compliance in e-government organizations in Saudi Arabia. Several hypotheses were formulated and assessed through statistical analysis with the data collected through surveys and questionnaires. The participants were professionals from E-Government organizations in Saudi Arabia.

From the results, it has been found that technical security controls are helping users to follow organizational security policies, thus fostering cyber security compliance. Similarly, accountability has a significant impact of users towards cyber security compliance and increased perceptions of accountability by employees deter security controls and policy violations. It is also evidenced that monitoring and control
has relationship and predicts compliance with policies by the employees. These are one of the factors that strongly effects the compliance behavior of the employees regarding security compliance.

By considering these factors, organizations and governments can better plan their cyber security strategies and cyber security investments. This can be accomplished by focusing on the key factors that directly affect employee security compliance and improve e-government security in public sector organizations. Once organizations understand the key cybersecurity compliance factors, they can create an enabling environment in which their employees can develop effective security compliance.

In future work, the remaining factors —Organizational commitment and End user awareness— will be assessed in the context of E-Government organizations in Saudi Arabia. These factors will also be assessed for stress inducing in employee and effects on user productivity.

**Declarations**

**Ethical Approval and Consent to Participant**

The ethical approval application was submitted to The University of Technology Sydney and obtained. The application included all the required consent to participant forms.

**Consent to Publication**

The consent to publication was obtained within the ethical approval application.

**Availability of Data Materials**

The data will be accessible by the researcher and his supervisor only and stored within the university polices.

**Computing interests**

Not applicable

**Funding**

Not applicable

**Author’s Contributions**

This study poses a number of theocritical and practical contributions towards user’s cyber security compliance behaviours in organizations. Both of them were discussed in detail above in this paper.

**Acknowledgments**

Not applicable
References

Ahlan, Abdul Rahman, Muhrman Lubis, and Arif Ridho Lubis. 2015. “Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures.” in Procedia Computer Science.

Al-Zahrani, Mohammed Saeed. 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.

Alharbi, Nawaf, Maria Papadaki, and Paul Dowland. 2017. “The Impact of Security and Its Antecedents in Behaviour Intention of Using E-Government Services.” Behaviour and Information Technology.

Almaiah, Mohammed Amin, Mahdi M. Alamri, and Waleed Al-Rahmi. 2019. “Applying the UTAUT Model to Explain the Students’ Acceptance of Mobile Learning System in Higher Education.” IEEE Access.

AlQahtani, Mohammed, and Robin Braun. 2020. “Assessing UTAUT2 Model for Cyber Security Compliance - A Literature Review.” Journal of Information Assurance & Cybersecurity.

Anon. 2010. “The Cambridge Dictionary of Psychology.” Choice Reviews Online.

Anthopoulos, Leonidas, Christopher G. Reddick, Irene Giannakidou, and Nikolaos Mavridis. 2016. “Why E-Government Projects Fail? An Analysis of the Healthcare.Gov Website.” Government Information Quarterly.

Avina, Glory Emmanuel, Kathleen Bogner, James Carter, Art Friedman, Susanna P. Gordon, Julie Haney, Linda Hart, Robert Scott Kittinger, Kiran Lakkaraju, In K. McCann, Ed Rhyne, and Dan Wolf. 2017. Tailoring of Cyber Security Technology Adoption Practices for Operational Adoption in Complex Organizations. Albuquerque, NM, and Livermore, CA (United States).

Balozian, Puzant, and Dorothy Leidner. 2017. “Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Asecurity Theory.” Data Base for Advances in Information Systems.

Bandyopadhyay, Kakoli, and Katherine A. Fraccastoro. 2007. “The Effect of Culture on User Acceptance of Information Technology.” Communications of the Association for Information Systems.

Barrane, Fatima Zahra, Gahima Egide Karuranga, and Diane Poulin. 2018. “Technology Adoption and
Diffusion: A New Application of the UTAUT Model.” *International Journal of Innovation and Technology Management.*

Bauer, Stefan, Edward W. N. Bernroider, and Katharina Chudzikowski. 2017. “Prevention Is Better than Cure! Designing Information Security Awareness Programs to Overcome Users’ Non-Compliance with Information Security Policies in Banks.” *Computers and Security.*

Boss, Scott R., and Laurie J. Kirsch. 2007. “The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines.” in *ICIS 2007 Proceedings - Twenty Eighth International Conference on Information Systems.*

Breaux, Travis D., Annie I. Anton, Clare Marie Karat, and John Karat. 2006. “Enforceability vs. Accountability in Electronic Policies.” in *Proceedings - Seventh IEEE International Workshop on Policies for Distributed Systems and Networks, Policy 2006.*

Brown, Susan A., and Viswanath Venkatesh. 2005. “Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle.” *MIS Quarterly: Management Information Systems.*

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.” *MIS Quarterly: Management Information Systems.*

Chang, Andreas. 2012. “UTAUT and UTAUT 2: A Review and Agenda for Future Research.” *The Winners.*

Chen, Xiaofeng, Liqiang Chen, and Dazhong Wu. 2018. “Factors That Influence Employees’ Security Policy Compliance: An Awareness-Motivation-Capability Perspective.” *Journal of Computer Information Systems.*

Chen, Yan, K. Ramamurthy, and Kuang Wei Wen. 2012. “Organizations’ Information Security Policy Compliance: Stick or Carrot Approach?” *Journal of Management Information Systems.*

Choi, Myeonggil, Jungwoo Lee, and Kumju Hwang. 2018. “Information Systems Security (ISS) of E-Government for Sustainability: A Dual Path Model of ISS Influenced by Institutional Isomorphism.” *Sustainability (Switzerland).*

Cialdini, Robert B., and Noah J. Goldstein. 2004. “Social Influence: Compliance and Conformity.” *Annual*
CommandHound. 2019. “Accountability Is Key to Security, Quality, and Compliance.” Retrieved (https://www.commandhound.com/accountability/accountability-is-key-to-security-quality-compliance/).

Cuganesan, Suresh, Cara Steele, and Alison Hart. 2018. “How Senior Management and Workplace Norms Influence Information Security Attitudes and Self-Efficacy.” Behaviour and Information Technology.

D’Arcy, John, and Gwen Greene. 2014. “Security Culture and the Employment Relationship as Drivers of Employees’ Security Compliance.” in Information Management and Computer Security.

D’Arcy, John, and Tejaswini Herath. 2011. “A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings.” European Journal of Information Systems.

Dempsey, K. L., Nirali Shah Chawla, L. A. Johnson, Ronald Johnston, Alicia Clay Jones, A. D. Orebaugh, M. A. Scholl, and K. M. Stine. 2011. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations.

Donalds, Charlette, and Kweku Muata Osei-Bryson. 2020. “Cybersecurity Compliance Behavior: Exploring the Influences of Individual Decision Style and Other Antecedents.” International Journal of Information Management.

Engotoit, Benard, Geoffrey Mayoka Kituyi, and Musa Bukoma Moya. 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.

Feigenbaum, Joan, James A. Hendler, Aaron D. Jaggard, Daniel J. Weitzner, and Rebecca N. Wright. 2011. “Accountability and Deterrence in Online Life (Extended Abstract)” in Proceedings of the 3rd International Web Science Conference, WebSci 2011.

Franke, Roland, Julia Kroenung, Friedrich Born, and Andreas Eckhardt. 2015. “Influential Factors for E-Government Success in the Middle East: Case Study Evidence from Saudi Arabia.” International Journal of Electronic Government Research.
George, Darren, and Paul Mallery. 2019. *IBM SPSS Statistics 25 Step by Step: A Simple Guide And Reference*.

Goodman, Seymour E., and Herbert S. Lin. 2007. “Enabling Accountability.” Pp. 113–26 in *Toward a Safer and More Secure Cyberspace*.

Griffith, Terri L. 1993. “Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring.” *Journal of Applied Social Psychology*.

Griskevicius, Vladas, and Robert B. Cialdini. 2010. “Social Influence.” in *Wiley International Encyclopedia of Marketing*. Chichester, UK: John Wiley & Sons, Ltd.

Haji-Tajuddin, Sharul T. Loughborough University. 2016. “The Role of ‘perceptions of Information Value’ in Information Security Compliance Behaviour: A Study in Brunei Darussalam’s Public Organisations.” Loughborough University.

Hanawalt, Christina. 2018. “School Art in an Era of Accountability and Compliance: New Art Teachers and the Complex Relations of Public Schools.” *Studies in Art Education*.

Harrell, Martha Nanette. 2014. “Factors Impacting Information Security Noncompliance When Completing Job Tasks.” *ProQuest Dissertations and Theses*.

Harris, Mark A., and Ronald Martin. 2019. “Promoting Cybersecurity Compliance.” Pp. 54–71 in.

Herath, Tejaswini, and H. Raghav Rao. 2009. “Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations.” *European Journal of Information Systems*.

Hochwarter, Wayne A., Gerald R. Ferris, Mark B. Gavin, Pamela L. Perrewé, Angela T. Hall, and Dwight D. Frink. 2007. “Political Skill as Neutralizer of Felt Accountability—Job Tension Effects on Job Performance Ratings: A Longitudinal Investigation.” *Organizational Behavior and Human Decision Processes*.

Hofbauer, David, Igor Ivkic, and Markus Tauber. 2019. “On the Cost of Security Compliance in Information Systems.” *10th International Multi-Conference on Complexity, Informatics and Cybernetics 2019 (IMCIC)*.

Hu, Qing, Tamara Dinev, Paul Hart, and Donna Cooke. 2012. “Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture.” *Decision Sciences*. 
Huang, Keman, and Stuart E. Madnick. 2020. “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, Allen C., and Merrill Warkentin. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study.” *MIS Quarterly: Management Information Systems.*

Karokola, Geoffrey, Louise Yngström, and Stewart Kowalski. 2012. “Secure E-Government Services.” *International Journal of Electronic Government Research.*

Kennedy, Prince, Modugu Emmanuel, and Famous Izedonmi. 2012. “Government Accountability and Voluntary Tax Compliance in Nigeria.” *Research Journal of Finance and Accounting.*

Kim, Sang Soo, and Yong Jin Kim. 2017. “The Effect of Compliance Knowledge and Compliance Support Systems on Information Security Compliance Behavior.” *Journal of Knowledge Management.*

Kolkowska, Ella, Fredrik Karlsson, and Karin Hedström. 2017. “Towards Analysing the Rationale of Information Security Non-Compliance: Devising a Value-Based Compliance Analysis Method.” *Journal of Strategic Information Systems.*

Koohang, Alex, Alojzy Nowak, Joanna Paliszkiewicz, and Jeretta Horn Nord. 2020. “Information Security Policy Compliance: Leadership, Trust, Role Values, and Awareness.” *Journal of Computer Information Systems.*

Krishnaraju, Vinodh, Saji K. Mathew, and Vijayan Sugumaran. 2016. “Web Personalization for User Acceptance of Technology: An Empirical Investigation of E-Government Services.” *Information Systems Frontiers.*

Lai, PC. 2017. “THE LITERATURE REVIEW OF TECHNOLOGY ADOPTION MODELS AND THEORIES FOR THE NOVELTY TECHNOLOGY.” *Journal of Information Systems and Technology Management.*

Lerner, Jennifer S., and Philip E. Tetlock. 1999. “Accounting for the Effects of Accountability.” *Psychological Bulletin.*

Li, Ling, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. 2019. “Investigating the Impact of Cybersecurity Policy Awareness on Employees’ Cybersecurity Behavior.” *International Journal of Information Management.*
Liu, Chenhui, Nengmin Wang, and Huigang Liang. 2020. “Motivating Information Security Policy Compliance: The Critical Role of Supervisor-Subordinate Guanxi and Organizational Commitment.” International Journal of Information Management.

Liu, Dapeng, and Lemuria Carter. 2018. “Impact of Citizens’ Privacy Concerns on e-Government Adoption.” in ACM International Conference Proceeding Series.

Lowry, Paul Benjamin, James Eric Gaskin, Nathan W. Twyman, Bryan Hammer, and Tom L. Roberts. 2013. “Taking ‘Fun and Games’ Seriously: Proposing the Hedonic-Motivation System Adoption Model (HMSAM).” Journal of the Association for Information Systems.

Marshall, Bryan, Robert Mills, and David Olsen. 2008. “The Role Of End-User Training In Technology Acceptance.” Review of Business Information Systems (RBIS).

Nanayakkara, Charith. 2007. “A Model of User Acceptance of Learning Management Systems : A Study within Tertiary Institutions in New Zealand.” The International Journal of Learning.

Pahnila, Seppo, Mikko Siponen, and Adam Mahmood. 2007. “Employees’ Behavior towards IS Security Policy Compliance.” in Proceedings of the Annual Hawaii International Conference on System Sciences.

Passyn, Kirsten, and Mita Sujan. 2006. “Self-Accountability Emotions and Fear Appeals: Motivating Behavior.” Journal of Consumer Research.

Ronchi, Alfredo M., and Alfredo M. Ronchi. 2019. “E-Government: Background, Today’s Implementation and Future Trends.” in e-Democracy.

S. Raschid Muller, and Mary L. Lind. 2020. “Factors in Information Assurance Professionals’ Intentions to Adhere to Information Security Policies.” International Journal of Systems and Software Security and Protection (IJSSSP) 11(1).

Salkind, Neil. 2012. Encyclopedia of Research Design.

Sanders, Debra L., Philip M. J. Reckers, and Govind S. Iyer. 2008. “Influence of Accountability and Penalty Awareness on Tax Compliance.” Journal of the American Taxation Association.

Sedikides, Constantine, Deletha P. Hardin, Kenneth C. Herbst, and Gregory J. Dardis. 2002. “Accountability as a Deterrent to Self-Enhancement: The Search for Mechanisms.” Journal of Personality and Social Psychology.
Shropshire, Jordan, Merrill Warkentin, and Shwadhin Sharma. 2015. “Personality, Attitudes, and Intentions: Predicting Initial Adoption of Information Security Behavior.” Computers and Security.

Silic, Mario, and Paul Benjamin Lowry. 2020. “Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance.” Journal of Management Information Systems.

Silverman, Henry. 2017. Research Ethics in the Arab Region. Springer, Cham.

Simonova, Alexandra (Capella University). 2020. “An Analysis of Factors Influencing National Institute of Standards and Technology Cybersecurity Framework Adoption in Financial Services: A Correlational Study.” Capella University.

Siponen, Mikko, Seppo Pahnila, and Adam Mahmood. 2014. Employees’ Adherence to Information Security Policies: An Empirical Study.

Sohrabi Safa, Nader, Rossouw Von Solms, and Steven Furnell. 2016. “Information Security Policy Compliance Model in Organizations.” Computers and Security.

Sommestad, Teodor, Henrik Karlzén, and Jonas Hallberg. 2019. “The Theory of Planned Behavior and Information Security Policy Compliance.” Journal of Computer Information Systems.

Šumak, Boštjan, Gregor Polančič, and Marjan Heričko. 2010. “An Empirical Study of Virtual Learning Environment Adoption Using UTAUT.” in 2nd International Conference on Mobile, Hybrid, and On-Line Learning, eL and mL 2010.

Taherdoost, Hamed. 2018. “A Review of Technology Acceptance and Adoption Models and Theories.” Pp. 960–67 in Procedia Manufacturing. Vol. 22. Elsevier B.V.

Toth, Patricia, Penny Klein, Patricia Toth, and Penny Klein. 2014. “A Role-Based Model for Federal Information Technology / Cybersecurity Training NIST Special Publication 800-16 A Role-Based Model for Federal Information Technology / Cybersecurity Training.” Nist Sp 800-16.

Twizeyimana, Jean Damascene, and Annika Andersson. 2019. “The Public Value of E-Government – A Literature Review.” Government Information Quarterly.

US Departement of Commerce. 2006. “Minimum Security Requirements for Federal Information and Information Systems.” Federal Information Processing Standards Publication.

Vance, Anthony, Paul Benjamin Lowry, and Dennis Eggett. 2013. “Using Accountability to Reduce Access Policy Violations in Information Systems.” Journal of Management Information Systems.
Vance, Anthony, Mikko Siponen, and Seppo Pahnila. 2012. “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory.” Information and Management.

Venkatesh, Viswanath, Michael G. Morris, Gordon B. Davis, and Fred D. Davis. 2003. “User Acceptance of Information Technology: Toward a Unified View.” MIS Quarterly: Management Information Systems.

Venkatesh, Viswanath, James Y. L. Thong, and Xin Xu. 2012. “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology.” MIS Quarterly: Management Information Systems.

Weerakkody, Vishanth, Zahir Irani, Habin Lee, Ibrahim Osman, and Nitham Hindi. 2015. “E-Government Implementation: A Bird’s Eye View of Issues Relating to Costs, Opportunities, Benefits and Risks.” Information Systems Frontiers.

Yazdanmehr, Adel, Jingguo Wang, and Zhiyong Yang. 2020. “Peers Matter: The Moderating Role of Social Influence on Information Security Policy Compliance.” Information Systems Journal.

Yen, Hsiu Ju Rebecca, Eldon Y. Li, and Brian P. Niehoff. 2008. “Do Organizational Citizenship Behaviors Lead to Information System Success? Testing the Mediation Effects of Integration Climate and Project Management.” Information and Management.

Yoo, Chul Woo, G. Lawrence Sanders, and Robert P. Cerveny. 2018. “Exploring the Influence of Flow and Psychological Ownership on Security Education, Training and Awareness Effectiveness and Security Compliance.” Decision Support Systems.