Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures

ARISTOTLE ONUMO, Computer Science, University of Bradford, United Kingdom
IRFAN ULLAH-AWAN, Computer Science, University of Bradford, United Kingdom
ANDREA CULLEN, Computer Science, University of Bradford, United Kingdom

The increase in cybersecurity threats and the challenges for organisations to protect their information technology assets has made adherence to organisational security control processes and procedures a critical issue that needs to be adequately addressed. Drawing insight from organisational theory literature, we develop a multi-theory model, combining the elements of the theory of planned behaviour, competing value framework and technology - organisational and environmental theory to examine how the organisational mechanisms interact with espoused cultural values and employee cognitive belief to influence cybersecurity control procedures. Using a structured questionnaire, we deployed structural equation modelling (SEM) to analyse the survey data obtained from public sector information technology organisations in Nigeria to test the hypothesis on the relationship of socio-organisational mechanisms and techno-cultural factors with other key determinants of employee security behaviour. The results showed that knowledge of cybersecurity and employee cognitive belief significantly influence the employees' intentions to comply with organisational cybersecurity control mechanisms. The research further noted that the influence of organisational elements such as leadership on employee security behaviour is mediated by espoused cultural values while the impact of employee cognitive belief is moderated by security technologies. For effective cybersecurity compliance, leaders and policymaker are therefore to promote organisational security initiatives that ensure incorporation of cybersecurity principles and practices into job descriptions, routines, and processes. This study contributes to behavioural security research by highlighting the critical role of leadership and cultural values in fostering organisational adherence to prescribed security control mechanisms.

Additional Key Words and Phrases: Cybersecurity, compliance, organisational culture, structural equation modelling

ACM Reference Format:
Aristotle Onumo, Irfan Ullah-Awan, and Andrea Cullen. 2020. Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Trans. Manag. Inform. Syst.* 1, 1, Article 1 (January 2020), 31 pages. https://doi.org/10.1145/3424282

1 INTRODUCTION

The International Telecommunication Union (ITU) described the cyberspace as the non-physical and interactive domain of information flow and communication between computer systems and networks. In other words, it is a global domain that consists of interdependent networks of information technology infrastructure including software and storage [4]. Over the years, organisations and governments have taken advantage of the non-physical domain to progress

Authors' addresses: Aristotle Onumo, A.O.Onumo@student.bradford.ac.uk, Computer Science, University of Bradford, United Kingdom; Irfan Ullah-Awan, Computer Science, University of Bradford, United Kingdom, I.U.Awan@bradford.ac.uk; Andrea Cullen, Computer Science, University of Bradford, United Kingdom.

from operating a dedicated network to a complex and decentralised interconnected system which have complicated security efforts by multiplying attack points. Securing this domain of interdependent networks have therefore become more complex with the increasing number of connected devices, thereby exposing organisations as potential targets of cybersecurity incident resulting in a huge financial and reputational loss[48].

Accordingly, recent studies have identified the human error and organisational insiders operating within the domain of the interdependent networks as among the major culprits behind most security breach either intentionally or unintentionally [48]. Compliance failure was also highlighted as one of the top factors responsible for the increasing cost of a data breach in public sector organisations. Equally other streams of research have demonstrated how insiders pose a great threat to the security of organisational information technology assets[8],[24] necessitating the need for an urgent response in order to address the risk posed by employees. Additionally, empirical evidence suggests that more information security incidents occur as a result of employee actions or inaction[54], explicating the necessity of a coordinated response to address the risk posed by organisational employee.

Behavioural information security research has emphasised on the need to address employee behaviour as a way of protecting and preserving confidentiality, integrity, and availability of organisations information at the cyberspace [20][14][11]. However, security measures incorporating both behavioural and technological approach have proved to be a more effective countermeasure [14]. Mitigating intentional and unintentional risk posed by the individual employee at the cyberspace, therefore, requires good corporate governance culture which results in the establishment of credible and reliable processes and a sound technical infrastructure among other standardized operational procedures.

One approach that could be considered is to ensure that individual employee follow established processes and procedure in information technology operations and adhere strictly to prescribed countermeasures in security management [11]. Numerous factors that could influence an individual employee to follow organisational processes and security control measures have been identified by various research streams [77]. Some studies have also identified compliance as one of the useful mechanism of influencing employee's behaviour when it comes to how organisation information technology resources are used[5],[35]. On the other hand when it comes to completing a task, [70] demonstrated that employees are likely to bypass security measures, while other studies have also identified security technologies such as public key infrastructure as a mechanism for compliance with organisational security procedure [83],[36],[74]. Scholars have equally suggested cybersecurity culture as a means of ensuring adequate protection and preservation of confidentiality, integrity, and availability of information at the cyberspace [14].

The focus of cybersecurity, therefore, is the individual or organisational response in the context of values and knowledge for the protection and preservation of information security principles within the operational space of the organisations' information technology infrastructure. Studies to increase our understanding of how the organisation, individual employee and operating environment interact to foster organisational cybersecurity compliance are important. For instance, we may want to know how certain organisational element interacts with cultural values to foster employee's security compliance behaviour.

Understandably, it was observed that security technologies constitute one of the key operational components that impact on employee security behaviour [83] [77]. However, the importance of and how such key constructs in the management and control of organisational security mechanisms influence security compliance have not been adequately examined. Furthermore, the combined effect of other sociocultural and organisational component that are the key constructs in the organisational and behavioural literature, have also not been adequately investigated. Therefore given the role of security technologies in ensuring compliance and the imperative of organisation culture and structure in shaping organisation compliance, studies on the single or combined effect of these constructs are needed to develop a better theoretical understanding and devise a more robust and effective means of fostering efficient security management through compliance to organisational cybersecurity control measures.

We attempt to address this gap in the literature by combining the theories of planned behaviour, technology organisation and environment with the competing value framework in what is referred to as the theory of integration [69] in order to understand how employee security behaviour could be adequately managed. We further attempt to address three critical questions which are yet to find adequate answers in the literature we reviewed. Firstly, How does the combined influence of organisational element such as leadership and other security behavioural mechanism foster the development of organisational compliance; secondly, how do organisational cultural values as measured by an organisational cultural assessment instruments (OCAI) influence organisational cybersecurity compliance ; and thirdly, what is the role of security technologies in fostering a positive employee cybersecurity compliance in the public sector.

Our focus on the role of security technologies in shaping employee cognitive belief makes this study distinct from others which rarely considers the technological environment in evaluating individual security behaviours. Furthermore by showing how organisational cultural values interact with other organisational mechanisms to facilitate compliant behaviour; we could offer management practical insight on the need to develop the right competencies and skills into addition to incorporating security goals into an organisational job routine.

The remainder of this paper is organised as follows; next is the review of some related works, section three is the information about the studies theoretical foundation. Our research model and hypothesis is presented in section four, section five contains the research methodology. Information about the analysis and result is presented in section six, section seven has discussion and implication for practice while conclusion and future works are presented in section eight.

2 REVIEW OF RELATED WORKS

2.1 Organisational Cybersecurity

Cyberspace security has become a key national and organisation discourse in view of its strategic role in maintaining the transforming impact of the digital economy as the world gradually move closer to the predicted 50 billion connected devices by the year 2020 [48]. While cyberspace is associated with numerous advantages, it, however, introduces risk to both the individual, organisations, and nations.

The concept of cyberspace security has been discussed by many authors and researchers alike. The comprehensive review of 19 nations cybersecurity strategies by [45] could not offer a common definition for cybersecurity from among the nations studied. While we do not aim at joining the discourse on the definition of cybersecurity, we shall, however, draw insight from scholarly presentations on the various perspectives of the concept as it suites our purpose and further progresses our study.

Some leading authors in the behavioural information security research describe cyberspace security (cybersecurity) as a process requiring a combination of tools and techniques applied by individuals and organisations to protect information technology assets and preserve the security principles of information contained and transmitted across interdependent networks with the aim of mitigating intentional and unintentional threat in the cyberspace [84],[13]. Others such the ISO/IEC 27032 describes cyberspace security as the protection and preservation of confidentiality, integrity, and availability of information in the cyberspace. However, the definition offered by ITU could suffice as a common understanding of many nations on the definition of cybersecurity. The organisation defined cybersecurity as the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practice, assurance and technologies that can be used to protect the cyber environment, the organisation and user assets [66]. We shall, therefore, adopt this definition for our study.

One globally recognised efforts towards institutionalizing the approach to cybersecurity is the formulation of cybersecurity strategies [45]. For instance, in Nigeria, the National Cybersecurity Strategy was launched by the National Security Adviser in 2014 with the overarching goal of providing a safe, secured, vibrant, resilient and trusted community that provides opportunities for its citizenry, safeguards national assets and interests, promote peaceful interactions and proactive engagement in cyberspace for national prosperity. However, the national cybersecurity strategies alone are only part of the process to the solution as it seeks among other things to establish a national governance culture that incorporates both individual and organisations in the application of control measures. These measures are designed to protect and preserve the confidentiality, integrity, and availability of information in the cyberspace through fostering the culture of security. It will, therefore, be beneficial to examine the perspectives of both individual and organisational behaviour while interacting with the cyberspace for effective cybersecurity management.

Organisational behaviour is about what individual do in an organisation and how their behaviour affects the performance of the organisation [61]. Furthermore, contextualising the definition of cybersecurity offered by ITU, we define organisational cybersecurity as the process of application of security concepts, principles and best practice technique for the protection and preservation of organisational cybersecurity infrastructure in accordance with structured prescriptions. What then emerges is the domestication of a culture of structured prescriptions on what to do and how to apply the various security concepts and best practice techniques within a group of people that have the common goal of protecting and preserving the cybersecurity infrastructure. This further results in compliance with organisations control measures in protecting the cyberspace in order to minimise and mitigate the loss of organisational data, which is the focus of this study.

2.2 Cybersecurity Knowledge

There has been a consistent debate in the literature on what knowledge is and what makes it organisational. While leading organisational Knowledge scholars described knowledge as being created by the flow of information, anchored in belief of the holder [51], other leading experts in knowledge management such as [16] defines knowledge as flux mix of framed experiences, values, contextual information, expert insight that provides framework for evaluating and incorporating new experiences and information. The authors further argued that knowledge originates and is applied in the mind of the knower and often becomes embedded in organisational processes, routines, practices, and norms. Practitioners however viewed knowledge as being synonymous with information [22].

We, therefore, draw insight from the various perspectives of knowledge presented by different experts and authors to conceptualise the definition of organisational cybersecurity knowledge that will serve the purpose of our study. The definition offered by [3] is apt in this regard. The author defined knowledge as the capacity to exercise judgment on the part of an individual which is either based on an appreciation of context or is derived from theory or both. Drawing insight from this definition, we disambiguate knowledge first by bringing contextual clarity on what is meant by the capacity to exercises judgment which according to [59] is the ability to draw distinctions, and secondly the context in which the criteria for evaluation holds which is the domain of practice (cybersecurity). We, therefore, conceptualise cybersecurity knowledge as the individual cognitive ability to understand their role in the security process and practical skills to rightly apply security control measures to minimize, mitigate and respond to the intentional and unintentional threat in order to protect organisational information technology resources. This definition preserves a significant role for human agency. For instance, individual computer user draws from among other things, sets of abstract instructions and guidelines such as ISO 27001 standards to mitigate and respond to an organisational threat to information technology assets. However, the policy on how these standards are applied to organisational practices makes this knowledge organisational. The distinguishing feature of organisation cybersecurity is, therefore, the generalisation of the behaviours by means of institutionalised prescriptions, functions and practices that are explicitly defined.

The protection of the organisation's network infrastructure and connected devices follows many processes which are predominantly dependent on human actions. Employee's lack of cognitive understanding of their security roles and responsibilities and absence of practical skills to rightly apply the controls are some of the major setbacks to the security of organisational information technology assets [12]. We, therefore, argue that employee security compliance behaviour is supplemented by the requisite cognitive ability and development of practical skills for the use and application of security technologies. An individual that lack proper cognition and practical skill on cybersecurity techniques and control will not have a refined distinction of appropriate application of security control measures in the organisation, whereas the incorporation of security control measures and procedures in the process of achieving organisational goal is an indication of how compliance to cybersecurity norms are valued as a strategic tool for organisational success. However, an organisation exists because of the presence of individuals or group who set out to achieve certain goals defined by sets of rules and cognitive beliefs [61]. There is, therefore, an apparent co-dependence between organisational elements such as leadership, employee cognitive mechanisms and cultural value of the organisation in fostering employee security behaviour in an organisation. An integrated approach to the study of these dimensions will, therefore, be useful and beneficial

Accordingly, the ISO/IEC/TRl 13335-1 2004, recommends that the protection and preservation of cyberspace infrastructure and resources require employees to share in the security vision of the organisation, understand their roles and responsibilities and develop practical skills to implement them. This is achieved through training the user on how to apply security controls, educating the employee on why such controls measures are necessary to be applied and creating awareness on their various role and responsibilities in the entire organisational security process. However, it has been argued that having the understanding of security roles and possessing practical skills to apply the control does to translate into compliance especially if it conflicts with employee's cognitive beliefs and cultural values [65]. This research, therefore, explores the link between organisational mechanisms, espoused cultural values and human action undertaken in an organisational context in an attempt to understand how security compliance could be better achieved; an area that has remained largely unexplored in extant literature.

2.3 Security Technologies

Security technologies refer to security mechanism deployed in establishing the requirements of organisational cybersecurity policies and standards in providing secured communication, protect IT assets and defence against attacks [83]. Security technologies coerce public organisation employee to improve their compliance with cybersecurity. Existing studies

have identified security technology as a factor that could propel the organisation to integrate cybersecurity in their work process in order to improve compliance [83]. Some empirical studies have also shown a direct link between the effectiveness of security technologies such Public-key Infrastructure (PKI), digital certificates and spyware technology and organisation compliance to cybersecurity requirements [72],[74] [36].On the other hand, [54] demonstrated that employees bypass security processes is an attempt to fast-track job completion.

With exception of one study [33], which merely identify leadership and security technologies as a factor that impact on employee security behaviour, no other study has been able to explore the interaction of cognitive belief mechanisms and security technology in the light of their impact on organisation security compliant behaviour. Besides identifying these constructs, studies on how they interact with other socio-organisational and cultural elements to shape cybersecurity compliance behaviour in an organisation have not been adequately investigated.

2.4 Organisational Leadership

Studies on information security have always focused on the employee as the weakest link in the defence. Arguably the action and inaction of the employee in correctly and incorrectly applying control measures and following prescribed procedures, principles and practices have a direct impact on the protection of the organisation's information technology infrastructure. However, despite the direct influence of this organisational element of leadership in promoting compliance and available literature in organisational leadership, empirical studies on how the organisational element of leadership comprise with employee security behaviour to foster security compliance have remained scanty [17]. Although many frameworks and behavioural models have been advanced to study security policy compliance, [56],[31],[25] are among the few that tested the role of organisational leadership with empirical data in an information security context. For instance, [56]found that there was a measurable change in employee attitude to security when the Chief Executive Officer (CEO) became more actively involved in information security issues. Also,[31] in their study found that top management participation strongly influences organisational espoused cultural values which in turn impacts employee attitude towards perceived behavioural control over compliance with information security policies. Other streams of research also emphasized the important role of management in encouraging positive behaviour towards the use of information system [37],[20].

The relationship between organisational culture and leadership have undoubtedly been studied by researchers on the assumption that organisational culture is created and managed by leaders [64],[2] and suggested that organisational success is premised on the ability of its leaders to effectively manage their culture. This assertion, however, forms part of the theoretical foundation of this study as according to [64] Leadership is associated with creation and management of culture.

2.5 Organisational Culture

Several scholars of organisational literature have defined culture in several ways. For instance, the functional view of [73] argued that culture conveys a sense of identity to organisational members, facilitates general commitment, enhances the stability of the social system and serves as an instrument of triangulation that shapes the behaviour of the members. In the author's view, organisational culture expresses the value of social identity and the pattern of belief that is shared by organisational members and manifested by symbols such as myth, rituals, stories etc. Another simple and well-known definition of organisational culture was provided by [46] The authors defined organisation culture as the way things are done here which in other word represents the identity and personality of the organisation [61], the author further opined that organisational culture is the social glue that binds the members which develop on the basis of what the organisation stands for. The author further argued that organisational behaviour is about what people do in an organisation and how their behaviour affects organisational performance, hence culture that evolves as a result of manifest behaviour is evident in the artefact, values, and basic assumptions.

The study by [31] identified organisational culture as one of the prime factors that promote security compliance. Additionally, the empirical research by [7] is among the few studies that tested the influence of organisational culture with empirical data in an information security context. The research operationalised and measured organisation culture in terms of cultural traits drawn from competing value framework of [57]. The authors linked the four cultural traits of cooperativeness, innovation (creativity), consistency, and effectiveness (Competitiveness) to four information security principles of confidentiality, integrity, availability and accountability in a structural model and found out that only effectiveness (competitiveness) and consistency have a significant effect on information security management principles. Besides, there is an apparent lack of empirical studies on the influence of organisation culture on employee security compliance behaviour as having been noted by some researchers [31], despite the obvious fact that organisational culture shapes organisational behaviour. Our study addresses this gap in the literature and contributes to theory development using an integrated approach.

2.6 Competing Value Framework

The Competing Value Framework of Organisational culture was proposed by Quinn 1988 to operationalise the shared beliefs and values which are assumed to be the manifestation of the underlying culture. This captures our definition of culture in terms of the values which represent manifestations that signify espoused belief identifying what is important to a particular cultural group in view of how things are done here [43]. The CVF has served as a useful tool for empirical study among cultural and organisational scholars[57]. It also provides a value-based framework for carrying out a quantitative inquiry about the role of organisation culture in an organisational setting. Though there are other cultural dimensions such as Hofstede six-dimensional framework, the five value cultural dimension by [34], we chose CVF in view of its wide application and tested empirical validity[57] [7].

Over the years the CVF has experienced a lot of reviews and has evolved with different labelling, though the basic characteristics of the framework remain the same. For the purpose of our study, we use [7] adaptation of Quinn 1988 original CVF with slight modification, though the essential characteristics remain the same as we believe that the modified adaptation is more supportive of our objectives.

In order to reduce the model complexity, and improve on the theoretical clarity given our task of integrating different theoretical frameworks, only two cultural value orientation in the lower half of CVF quadrant is considered. This is also supported by the outcome of an empirical investigation by [7]. The authors tested the relationship between the four cultural value and the four constructs of information security management principles and found that the cultural values related to control (consistency) and competitiveness (effectiveness) have a significant impact on information security management principles

2.7 Employee Security Compliance Behaviour

Several studies have examined employee's behavioural compliance in an organisation. Majority of these studies which drew from Protection Motivation Theory, Theory of Planned Behaviour, or Cognitive theory have focused primarily on factors related to users attitude, intentions, and behaviours. For instance, [35] combine the theory of Planned behaviour and Protection Motivation Theory to show that perceived vulnerability, response efficacy, self-efficacy, attitude towards compliance with information security policy and subjective norms influence the intention to comply. Similarly, studies were also conducted by [65] using protection motivation theory to show that visibility, normative belief and threat appraisal impact on the intention to comply with ISP. [28] validated an integrated model to gain insight into the behavioural norm, attitude and motivation that affect employee intention. The authors combine PMT, Deterrence Theory and decomposed TPB to show that perceived severity has a significant effect on users attitude to comply with security policies. It further demonstrates the impact of organisational commitment on the intention to comply. The principle of the rational choice theory was also used to study the impact of the antecedent of attitude on the intention to comply with ISP [5]. This study also found out that attitude, normative belief and self-efficacy have a significant effect on the intention to comply with Information Security Policies. The study by [86] also shows that employees intention to comply with security policies might be weakened if such employee is perceived that there is strong technical protection to secure organisations information technology assets. In a related study, [69] combined elements from PMT, TRA, and cognitive evaluation to develop a multi-theory model that explains employee's adherence to security policies. [19] empirically validated an integrated model to gain insight into the implication of organisational element of leadership and cultural trait in managing employee compliance to information security. The author concluded that top management strongly influences organisational culture which in turn impacts employee cognitive beliefs towards information security compliance.

Various studies in behavioural science and information security have rendered strong support that individual attitude, subjective norm and perceived behavioural control significantly influence individual behavioural intention. It has been demonstrated that individuals are more likely to pursue endeavours that they perceive as having a positive outcome in their life[47]. Researchers have also recommended these combined construct as a tool and intervening factors that influence organisational behaviour. For instance, [54] in well-validated research examined the relationship between the combined constructs of training, education and awareness and employee security behaviour and concluded that employee knowledge of security policy and the procedure has a strong influence on attitude towards the policy and procedure. This result further confirmed an earlier assertion by Knowledge, Attitude and Behaviour (KAB) model [39],[42] supporting the influence of intervening factor in organisational security behaviour. Our theoretical research also reveals that the adherence to organisations cybersecurity principles and practices requires the employee's cognitive evaluation and understanding of their various roles and responsibilities in the organisations security formation and develop practical skills to apply them as it has been shown that both interest and the perceived outcome has impact on the choice of action[47].

2.8 Theory of Integration

Integrating theories from different theoretical field domains bring in dynamism and ideational clarity and support needed for the fostering of organisational security practice and compliance in view of the multidisciplinary nature of cybersecurity. It is based on approaches, practices and associated construct of different theories brought in a hybrid nomological network. The concept builds upon existing conceptual knowledge to create a robust model with a broader scope, [13] [40], better explanatory power[69]. According to [40], participating theories are selected on the basis of epistemic compatibility, construct commonality, theoretical complementarity and conceptual harmony. In addition, [30] identified three modes of integrating different theoretical domains especially as it relates to information systems as construct integration, domain integration and inter-field integration. While our approach to inter-field integration relies on the preconditions as suggested by Koch [40], the research, however, adopted [30] proposition in explaining the rationale behind the theoretical choices for integration where one field consist of distinct entities that do not explicitly exist in the other field. The research considers culture to provide the basis of commonality among the participating theoretical field domains [31] especially in the information security domain which has been conceptualised as a complex and dynamic evolutionary process.

Additionally. the different theoretical field of the theory of planned behaviour, Technology-Organisation and Environment theory and organisation cultural framework share a common interest in explaining employee security behaviour in an organisational context [30]. Contextualising [30] propositions, our research assumes the operational location of the theory of planned behaviour is provided in the organisation and its culture and that the properties such as employee's cognitive belief mechanisms for which the organisation and its culture postulates is identified in the theory of planned behaviour. Accordingly, [30] suggests that for inter-field integration, the different theoretical domains may determine structures of entities whose functions are the domain of other theoretical fields. For instance, employee security behaviour is the focus of the organisation's structure but compliance belongs to the domain of cognitive belief and culture. The foregoing therefore present the research suitable for adoption of the theory of integration in explicating organisational security practice and compliance.

2.9 Theoretical Gap

Our literature review reveals major theoretical gap which our study intends to fill. First, the important role of culture in cybersecurity have been studied by some scholars [53], however as [31] observed, such studies are not only lacking strong theoretical foundation but also empirical evidence on overall effectiveness. It is not also clear how culture is influenced either directly or indirectly by other organisational mechanisms to foster organisational security compliance. Secondly, the impact of security technologies in facilitating organisation compliance is yet to receive adequate attention. Although the case evidence provided by [33] mainly established security technology as a factor, it is not clear on how such a relationship will impact on organisational compliance with cybersecurity requirements. The important influence of leadership in fostering organisational compliance to cybersecurity control measures has not received adequate attention. Out of all the literature reviewed by the researcher, it was only the study by [33]and [25] that provided theoretical support in examining the influence of organisational leadership in enhancing security compliant behaviour. Although the call for a more holistic information security management approach comprising of the technological, organisational and social component has resulted in the witnessed increase in the investigation of employee security behaviour and compliance, most studies, however, have focused primarily on identifying factors related to individual attitude and organisational behaviour [35]. Additionally, behavioural information security researchers have suggested compliance and cross-cultural approach as possible areas to explore in addressing the predominantly weakness in securing the organisation's information assets[11]

Despite strong evidence linking organisational elements of leadership, organisation culture and employee cognitive belief mechanisms to compliance, empirical studies on how these factors interact to foster organisational compliance with security requirement have remained scanty. Articulating and testing the combined effect of such organisational mechanisms on employee security behaviour will fill a major gap and contribute to the theory and practice of information security management.

3 RESEARCH MODEL AND HYPOTHESIS

Belief constructs such as attitude and subjective norms which is thought to have an influence on individual behaviours have remained the focus study among many scholars of industrial psychology and behavioural science [13],[1]. Streams of research and extant literature show that organisational structure and environment, development of skills and promoting security policies and mechanisms shapes employee behaviour [20].[62],[69] [10].

To fully understand the employee security behaviour in an organisation, the socio-organisational and techno-cultural context such that promotes the development and understanding of how to apply the security technologies for satisfying organisational cybersecurity control measures and standards must be accounted for. Accordingly, we propose that integrating various theoretical frameworks to analyse the impact of cognitive belief mechanisms will provide more guided explanation and increase our understanding of the core determinant of the employee willingness to comply with organisational security requirements. We there argue that fostering organisational security compliance requires the direct participation of individual or group within the organisation with the vision of promoting adherence to cybersecurity principles and practices as a value to be incorporated in the organisational job description, processes and routines. This logic is illustrated by our conceptual model in Fig 1. Our focus on clarifying the influence of leadership and other organisational mechanisms on employee cognitive belief in fostering cybersecurity compliance and how this influence is moderated by security technologies constitute the major contribution of this study.

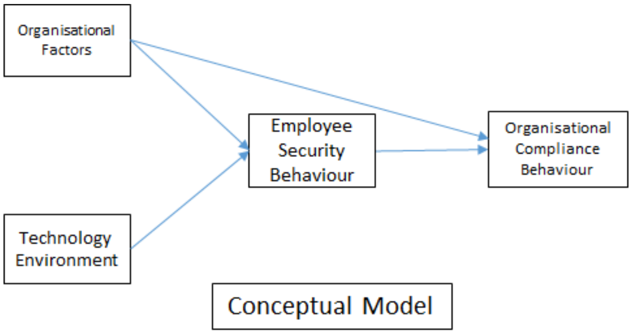
Organisational Factors
Employee Security Behaviour
Organisational Compliance Behaviour
Technology Environment
Conceptual Model

Fig. 1. Conceptual Model

3.1 Theories and Research Model

Theory of Planned Behaviour (TPB) has been found to be useful in predicting behaviour. It suggests that the stronger the intention to engage in behaviour of interest, the more likely hood to perform the behaviour. The intention, on the other hand, refers to factors that motivate individuals to carry out an action. According to [1], the intention is determined by the attitude towards the behaviour, subjective norm and perceived behavioural control. Attitude is defined as a person's judgment as to whether it is good or bad to perform a behaviour of interest, in the case of subjective norm, it is described as the persons perception of whether the behaviour of interest is accepted and encouraged by people who are important to him/her such as colleague, subordinates or superiors in an organisational setting. Perceived behavioural control is explained as the perceived ease or difficulty in promoting or performing a behaviour of interest [1]. Accordingly, the construct which is the third component of TPB and is further described as a person's expectation that the performance of the behaviour of interest is within his/her control. Conceptually, both PBC and Badura's Self Efficacy are similar [85] as they operationally refer to the ease or difficulty of performing or facilitating a behaviour of interest. Additionally, the judgement of PBC is influenced by the belief concerning access to necessary resources and opportunity to successfully perform a given task or behaviour of interest [1]. These factors likely to facilitate or inhibit the performance of a given behaviour of interest are referred to as control beliefs factors which include individual cognition, capacity and competence to cope with a task or make choice (Badura 1991) and they are weighted by its perceived power to facilitate or inhibit the performance of a behaviour[1]. For instance, it is assumed that when one has the intention to perform a given security behaviour or task and fails to act on the intention, the failure is attributable to the absence of control over the behaviour of interest due to lack of cognition, skill or opportunity [26]. In Information security, therefore, such locus of control considered to be component of PBC [1] describes individual cybersecurity knowledge and expertise that facilitate the performance of their security task or given security behaviour [71],[82]. For the purpose of the study, we replace PBC with cybersecurity knowledge as it is well suited for our study as a component of PBC that will control compliance to specific security task or behaviour of interest [24],[21]

3.2 Research Hypothesis

The cybersecurity knowledge has earlier been conceptualised as the cognitive ability to understand roles and responsibilities and the presence of practical skills for the right application of security control and measures to satisfy the requirement of organisational cybersecurity. This is achieved through training, education and awareness [75],[50]. We adopted this proposition to ensure the reliability and internal consistency of our construct measures. It therefore logical for us to propose that;

H1: *The increased prevalence of knowledge of cybersecurity in an organisation will positively influence the employee's intention to comply with cybersecurity control measures.*

H2: *Positive attitude to the requirements of cybersecurity control measures increases employees intention to comply.*

H3: *Employees subjective norms positively influence their intention to comply with cybersecurity control measure.*

Individual behavioural intention affects the likelihood that such behaviour of interest will be performed. In other words, intentions are motivation for a particular behaviour of interest to occur. Drawing from the theory of reasoned action, [1] developed the theory of planned behaviour, proposing that peoples cognitive evaluation of behaviour should lead to higher intentions. In line with suggestions of many researchers urging IS scholars to include actual behaviour in their research [44], we adopt the concept of intention and actual behaviour in our model so as to make both explicit [63],[35] while incorporating the propositions of the theory of planned behaviour in the context of cybersecurity compliance. It is, therefore, a straightforward logical deduction for us to propose that;

H4: *Employees intention to comply with cybersecurity control measures will positively influence their actual compliance.*

One of the most important outcomes of the influence of organisational elements such as the active participation of leadership in an organisation is how the latter impacts on both organisational culture and individual cognitive beliefs. According to [64], beliefs, values, and assumptions of the founding fathers of the organisation are one of the primary sources through which organisational culture evolves. These beliefs, values, and assumptions are reinforced by the leadership by putting measures in place to, monitor, and control, manage and allocate resources in order to achieve organisational goals. Leadership, therefore, is the process of influencing a group of individuals to achieve a common goal[52].

How this important organisational element conspires with culture and individual cognitive belief mechanisms in influencing the outcome of Information system implementation has been established in works of literature [37]. By articulating visions and strategies and setting goals and at the same time developing programs, initiatives, policies, structures and training to ensure proper alignment, leadership shapes the values, beliefs and basic assumptions of the organisation. Studies have also shown that if employers can provide a set of security guidelines, develop the knowledge of the employee in understanding and practical application of security controls and strictly monitor employees, information security compliance will also improve [20]. Another stream of research has also shown that subjective norms, attitude and perceived behaviours control are also influenced by the organisational security policy, guidelines and measure which defines the direction of leadership commitment to cybersecurity [62]. We, therefore, propose that;

H5a: *The participation of leadership in the structuring of cybersecurity initiatives and programmes impacts positively on employee attitude towards organisational cybersecurity compliance.*

H5b: *The participation of the leadership in the structuring of cybersecurity initiatives and programmes positively impacts on subjective norms about organisational compliance to cybersecurity control measures.*

H5c: *The involvement of leadership in the structuring of cybersecurity initiatives and programmes positively impacts on organisational cybersecurity knowledge.*

Organisational leaders can re-enforce the espoused values of how things are done here through monitoring, controlling, allocating resources, teaching, coaching, allocating rewards etc [64]. According to [38], direct involvement and participation of the leaders in one of the cultural dimensions influence the employee involvement in that direction. For instance, it is expected that the participation of leadership through the development of initiatives and strategies ensuring the incorporation of organisation's security goals in job descriptions, processes and routines will directly impact on the relevant cultural values that have to do with the task to be done or the rules to follow in accomplishing the task. The organisation is set on the competitive mode when the focus is on the task and on the (control) consistency mode when the interest is biased to the rules to be followed [57]. This will in effect send a strong signal of legitimacy and increase the employee value for such a mechanism of influence. We can, therefore, postulate that;

H6a: *The direct participation leadership in the structuring of cybersecurity initiatives and programmes will positively impact the rule orientation cultural value.*

H6b: *The direct participation of leadership in the structuring of cybersecurity initiatives and programmes will positively impact the task-oriented cultural value.*

Technology-Organisation and Environment (TOE) theory have been found to be useful in investigating the socio-organisational factors affecting organisational compliance with security requirements. The theory argues that the process by which technological innovation is adopted and implemented in an organisation is conspired by the technological, organisational and environmental context surrounding their operations [18]. This study focuses on assessing the effect of security technologies on employee security behaviour (the relationship between intention to comply and actual compliance). It regards the security mechanism deployed for establishing the requirement of organisational cybersecurity policies and standards as innovation decision. For instance when public key infrastructure is deployed to enhance compliance, such is regarded as innovation-decision, a tool analogous to information communication technology adoption[18]. In this regard, TOE, therefore, offers, a more holistic view of security technology application.

We define technology in the context of TO-E as the reliability and relative advantage of security technologies in satisfying the requirements of security control measures and standards [83]. In other words how the presence of security technology will conspire with the employee intention in taking security decision[58]. This study, however, considers the security technology component of the TOE as a mechanism which moderates employee security compliant behaviour. The research further assumes leadership as an organisational element which conspires with individual cognitive belief mechanisms to shape security compliance. Since the research was conduct in a public sector technology environment that is already ISO/IEC/ISMS/27001 certified. It is therefore legitimate to propose that;

H7: *Employees intention to comply with cybersecurity requirements is moderated by the application of security technologies.*

Furthermore, we define cybersecurity compliance behaviour as conforming to existing rules, processes, procedures, and standard in performing the task of the protection of organisations computer networks and information technology assets; in other words, follow the rules to perform the task. It is therefore evident from the definition that the two important cultural values that shape the security-related behaviour of the employee are; conforming to rule and completing the task. A rule-based cultural orientation reflects the control of organisational processes and procedure through a bureaucratic/hierarchal structure, individual consistency, and uniformity in following procedures and processes. As a manifest value of such culture, the employee's roles will be formally defined and documented while stability is achieved within the organisation through effective information management [56]. While studies in organisation culture have suggested a significant direct linkage between the cultural values and behavioural intentions of the employee [79] there are however limited research works on the effectiveness of rule-oriented culture in shaping employees cognitive beliefs in an organisation. Although as an espoused cultural value, it is expected that a rule-based culture will have a similar effect on employee cognitive beliefs as that of culture in general in the context with organisational compliance. For example in a bureaucratic organisation where employee view compliance to rules positively, it is reasonable to assume that fostering compliance to cybersecurity control measures will be organisational norm, hence the likelihood that a particular security behaviour of interest will be carried out.

A task-based cultural orientation reflects a collective understanding of organisational goals as embedded in the individual task, individual responsibility, and accountability. The manifest value underlying such culture is task completion, goal achievement while competition and profitability become a measure of organisational efficiency and productivity [57]. Drawing from the definition of our outcome variable which is about conforming to prescribed cybersecurity procedures and control measures, we can reasonably conclude that in task-based cultural value organisation, the likelihood that a particular security behaviour interest will be performed is weakened by the focus on task performance and goal achievement. We, therefore, propose the following;

H8a: *A rule-based oriented cultural value positively influence employee intention to comply with cybersecurity control measures*

H8b: *A rule-based oriented cultural value positively influence employee actual compliance with cybersecurity control measures.*

H8c: *A task-based oriented cultural value weakens employee intention to comply with cybersecurity policy requirements*

H8d: *A task-based oriented cultural value weakens employee actual compliance with cybersecurity security control measures.*

4 STUDY DESIGN AND RESEARCH METHOD

The study combined the Theory of Planned Behaviour (TPB) Technology Organisation Environment theory and organisational cultural framework to conceptualise cybersecurity compliance model. We need to understand why an employee exhibit various level of commitment and sense of responsibility and how leadership as an organisational element interaction with other cognitive and behavioural mechanisms to foster compliance with cybersecurity procedure and control measures. To achieve this, information was collected from a review of works of literature to conceptualise the initial model in Fig 1. The logical relationship between the various constructs was later developed in proposing our hypothesis as summarised in the research model (the structural path Fig2).

Measurement items for each construct in the model were based on a five-point Linkert scale. All the survey items have been used and tested in earlier studies and were adapted for use in the current study. In addition, since the measures have not been tested in the context of security compliance especially in Nigerian public sector information technology organisation, our analysis further tested the reliability and validity of these measures. The construct and their primary source are listed in Table 1 while the survey instrument and test of validity are found in Table 3 and 6.

Table 1. Construct Operationalisation

Construct	Definition	Theoritical Framework	Primary Source
Leadership	The presence of individual who influences a group of individual to achieve a common goal	Achievement Motivation Theory of Leadership	[49] and Boyatzis, R.E., 1982, [2] [30]
Goal Oriented Cultural Value	Values espoused by employee in the belief that performance and appraisal are directly related to the attainment of organisational goals clearly defined by leadership	Cultural Value Framework (CVF)	[57], [81]
Rule Orientate Cultural Value	Espoused values by the employee in the belief that jobs and tasks are performed according to job specifications and clearly defines procedure by everyone in the organisation	Cultural Value Framework (CVF)	[57], [81]
Cybersecurity Knowledge	Individual cognitive ability of understand their role in the security process and practical skills to rightly apply security control to minimize, mitigate and respond to intentional and unintentional threat in order to protect organisational information technology resources	Theory of Planned Behaviour (TPB)	[12]. [78]
Attitude	Judgement as to whether it is good or bad to perform a behaviour of interest	Theory of Planned Behaviour (TPB)	[1], [5]
Subjective Norm	Belief of whether a behaviour of interest is accepted and encouraged by people who are considered impotent and influential in the organisation such as subordinates or superior	Theory of Planned Behaviour (TPB)	[1], [5]
Behavioural Intention	Belief that a behaviour of interest will be performed sometime in the future	Theory of Planned Behaviour (TPB)	[1], [5]
Compliance	conforming to existing rules, processes, procedures and standard in performing a task		Vroom 2004
Security Technologies	Security mechanism deployed in establishing the requirement of organisational cybersecurity policies and standards in providing secured communication, protect IT assets	Technology –Organisation and Environment (TOE)	Wimmer and Von Bredow 2002, [83]

4.1 Data Collection

Measurement items for the survey instrument were refined through a pilot study using 20 participants selected through key informant method and mainly from among the senior staff of the National Information Technology Agency and National Planning Commission in Nigeria.

According to [67], the key informant methodology advocates that respondents should be identified based on their position, and professional knowledge rather than by traditional random sampling. During the pilot test, the key informant included chief scientific officers, senior scientific officers, and principal officers. We observed some reluctance in completing the questionnaire and the clarifications sought by the respondents. Based on the feedback, we revised the questionnaires, reduced the number of items and rephrased some sentences to increase comprehension.

The final version of the questionnaire used for the study included 62 questions in which every construct was measured by various items. We used paper-based questionnaires which have been noted to improve response rate. In order to speed up the process of data collection and decrease the number of incomplete responses, we instantly reviewed responses and kindly requested the respondent to reply to the neglected questions. This approach eventually paid off as only two questionnaires (1.6 per cent) were rejected during the analysis as a result of the incomplete response.

The key informant method was also adopted in selecting the participating agency, we first wrote the heads of these agencies to obtain their permission to participate in the main survey and followed it up with visits to clarify the purpose of the survey and solicit their quick and honest response.

A total of 300 questionnaires were distributed among the key informant which included Chief Scientific Officers, Chief Information Security Officers, directorate level officers, out of which 122 were retrieved, a response rate of 40.7 per cent which is relatively high when considered the concept being researched on [35]. The descriptive statistics in Table II shows that about 62 per cent of the respondents are male while 38 per cent are female. It further reveals that about 60 per cent have served in their organisations for more than 5 years and all the participants have a minimum qualification of first degree (Table (2). The public sector information technology organisations comprising of National Information technology Agency (regulatory), Galaxy Backbone (IT Infrastructure service provider) and National Identity Management Commission (IT application service user) participated in the survey.

In view of the sensitivity of the information sought, additional safeguard measures were put in place to preserve the anonymity of the respondent while at the same boosting their confidence to participate in the survey. To this end, our survey items were reviewed and approved by University of Bradford ethics and review board who also directed that the approval statement should be included as a footnote at every page of the survey item. As part of additional measure to protect the respondents, we also ensured that none of the survey items contained any personally identifiable information.

5 RESULTS

Partial Least Square Structural Equation Model (SEM) was used to test the measurement models psychometric properties and structural model. We use the variance-based PLS-SEM instead of covariance-based in view of the following reasons; (1) PLS-SEM does not require large samples [27]. Research has shown that it offers a better estimate than other technique for sample size under 250 [41][80] (our sample size is 120). Secondly, the techniques are better suited for non-normally distributed data [27] [68] [23]. Smart PLS [60] was used as a major statistical tool for model estimation using a two-step approach. First, we assess the quality of the measurement model to ensure the validity and reliability of items and finally, the structural model was analysed in order to test the hypothesis and the quality of the structural model.

Table 2. Descriptive Statistics of the Respondents

Category	Subcategory	Frequency	Percentage
Gender (N=120)	Male	74	61.7
	Female	46	38.3
Years of Experience	Less than 5 years	43	35.8
	5-10years	50	41.7
	Above10years	22	18.3
Edu. Qualification	Bsc	60	50
	Masters	55	45.8
	PhD	2	1.7

5.1 Quality of Measurement model

The quality of the measurement model is usually assessed in terms of its content validity, construct validity and reliability. This is to ensure that only reliable and valid construct measures were used for assessing the nature of relationships in the overall model [32]. Content validity reflects the extent to which the items represent the construct being measured and is usually assessed by domain experts. In our study, this is achieved by adopting previously published measurement items for the construct and feedback from our pilot study. Construct validity for our reflective measures defines the degree to which the measurement items are related to the construct to which they are theoretically predicted to be related. The validity of the constructs was assessed through internal consistency, indicator reliability, convergent reliability, and discriminant validity.

Table 3. Fornell and Larker Discriminant Validity

Construct	CR	CA	AVE	ATT	COM	COMP	CON	INT	KNO	LEA	SUB-N
ATT	0.880	0.809	0.656	0.81							
COM	0.905	0.875	0.615	0.249	0.784						
COMP	0.901	0.763	0.821	0.612	0.288	0.906					
CON	0.895	0.860	0.589	0.477	0.533	0.504	0.797				
INT	0.874	0.811	0.635	0.643	0.137	0.590	0.341	0.797			
KNO	0.908	0.880	0.623	0.467	0.271	0.531	0.466	0.454	0.790		
LEA	0.902	0.855	0.679	0.389	0.335	0.419	0.503	0.270	0.748	0.835	
SUB-N	0.880	0.809	0.589	0.352	0.233	0.361	0.259	0.458	0.350	0.278	0.768

[21] recommended indicator outer loading of 0.708 for the reliability of the reflective measure to be established. The authors further suggested that indicators outer loading between 0.4 and 0.7 should be considered for deleting if only it will lead to an increase in composite reliability above the recommended threshold. After running the PLS algorithm we dropped items COMP3 and COMP4, KNO4 and KNO5 because the items were below the level of acceptable indicator reliability threshold. We retained item ATT4, COM-C2, and SUB-N4, since dropping then did not affect the reliability of our construct measures [27]. See Table 6 for indicator outer loading

Convergent validity refers to the degree of agreement in two or more measures of the same construct and is assessed by inspection of variance extracted for each factor [21] Accordingly, convergent validity is established when the Average Variance Extracted (AVE) yield a value above 0.5. Looking at table 3, we can see that all AVE values were above the threshold, we can, therefore, conclude that convergent validity is ensured. According to [27], adequate internal consistency and reliability are established when Fornell and Larckers measure of composite reliability and Cronbach alpha is higher than 0.7 The Composite Reliability (R and Crombach Alpha (CA)values in Table (3) are all above 0.7 suggesting adequate internal consistency. Discriminant validity refers to the extent the measures of different constructs are unique; ie the degree to which a single construct is different from the other constructs in the model[6].

This is achieved when two conditions are fulfilled using the test provided by [21]. First, when the constructs have AVE loading greater than 0.5 meaning that at least 50 per cent of measurement variance was captured by the construct [Chin 1988] and secondly when the square root of each constructs AVE is higher than the correlation with any other construct. As Table 3 shows, the square root of the constructs AVE is higher than the correlation with any other construct, Tables (3) and (6) shows that the constructs possess discriminant validity.

The threat of common method bias was addressed by ensuring the anonymity of respondents, requesting that each question should be answered as honestly as possible and by not providing an incentive for participation in the study. In addition, we placed the demographic questions at last to reduce fatigue. All data tested suggest that the items are both valid and reliable and thus could be used to evaluate the structural model.

5.2 Evaluation of Structural Model

Structural Equation Model (SEM) comprised of statistical methods to test the hypothesised relationship in a conceptual or theoretical model. It explores relationships between dependent, independent, moderation and mediating variables. SEM has the ability to isolate observational errors from the measurement of latent variables and this attribute has made the tool to be widely applied in various research areas[27].

The SEM in Fig (3) presents information about hypothesised relation using path co-efficient Beta and R squared. Beta denotes the strength of the path coefficient (hypothesised relationship) while the R squared values of the endogenous constructs measures how variance in the endogenous variables are explained by the exogenous variables specified in the model [59]. Because PLs does not require a normally distributed data, it is evaluated with R squared calculation for dependent latent variables [9] which determines how well the model fits its hypothesised relationship and constructs percentage variation that is explained by the model. According to [Chinn 1988] R squared value of 0.67, 0.33, and 0.19 can be described as substantial, moderate or weak. R squared value for the dependent variable; Compliance is 0.46, indicating that the variables in the model explained about 46 per cent of the variance in the dependent variable. Thus the proposed structural model could be said to have strong explanatory power and explains a substantial amount of the variance in actual compliance to organisational cybersecurity policy requirements especially when compared with similar published studies (eg 42 per cent in [29], 35 per cent in[5], 30 per cent in [15]

Additionally, the structural model can also be assessed using effect size ie F squared [9], Goodness of Fit [55] and predictive relevance; Stone-Geisier Q squared. According to [9] F squared value of 0.02, 0.15, 0.35, signifies small, medium and large respectively. The goodness of fit which represents the index of validating PLS model [76] was employed to judge the overall fit of the model by presenting a compromise between the performance of the measurement and structural model. The GoF is calculated as the geometric mean of the average communality and average R squared normalised between 0 and 1, where a high value indicates better path model estimation. For this model, the GoF index was 0.43. The Q statistics measure the predictive relevance, a model is said to have predictive relevance if Q squared is greater than zero and lacks predictive relevance if Q squared is less than zero [21]. In PLS, two kinds of Q statistics are estimated using blindfolding methods of calculations. Our results reveal that for this model, all the blocks had high values of cross-validated communality ranging from 0 to 0.59 and cross-validated redundancy ranging from 0 to 0.327. All the values are positive meaning that the model is structurally sound as possesses acceptable performance and predictive relevance.

Table 4. Result of Hypothesis Testing

Path	Beta	SDEV	T Stat.	P Values	F^2	Result
ATT>>INT	0.500	0.097	5.166	0.000	0.247	Accepted
COM>>COMP	0.056	0.084	0.669	0.504	0.008	Rejected
COMP>>INT	0.096	0.098	0.984	0.325	0.025	Rejected
CON>>COMP	0.311	0.096	3.249	0.001	0.101	Accepted
CON>>INT	0.020	0.103	0.192	0.848	0.005	Rejected
INT>>COMP	0.476	0.097	4.911	0.000	0.372	Accepted
KNO>>INT	0.151	0.077	1.954	0.051	0.034	Accepted
LEA>>ATT	0.389	0.100	3.901	0.000	0.185	Accepted
LEA>>COM	0.335	0.088	3.797	0.000	0.134	Accepted
LEA>>CON	0.503	0.074	6.756	0.000	0.338	Accepted
LEA>>KNO	0.748	0.039	19.11	0.000	1.275	Accepted
LEA>>SUB-N	0.278	0.105	2.659	0.008	0.102	Accepted
SUB-N>>INT	0.247	0.095	2.601	0.009	0.099	accepted

In order to assess the significance of the structural path, bootstrapping re-sampling with 120 cases and 1000 re-samples were used [Chinn 1988. The result of the hypothesis test is presented in table (4). All the hypotheses in the model are supported by our data except the path of the cultural values to intention to comply and the path of task-oriented culture to actual compliance. All the hypothesis related to the theory of planned behaviour is strongly supported by our data at 0.05 per cent significance level, confirming the resilience and reliability of the theory in predicting individual behaviour in a socio-organisational environment. The two hypotheses linking the cultural values of task and rule orientations to intention to comply is not supported by our data. This is not surprising since, by our definition of organisational culture, it extols the important espoused values individual employees are expected to comply with and does not evaluate their willingness or commitment to those values. Little wonder why the hypothesis is not supported by our data and yet the same cultural values have a significant impact on actual compliance. However, this result is consistent with the ones obtained in extant literature [31].

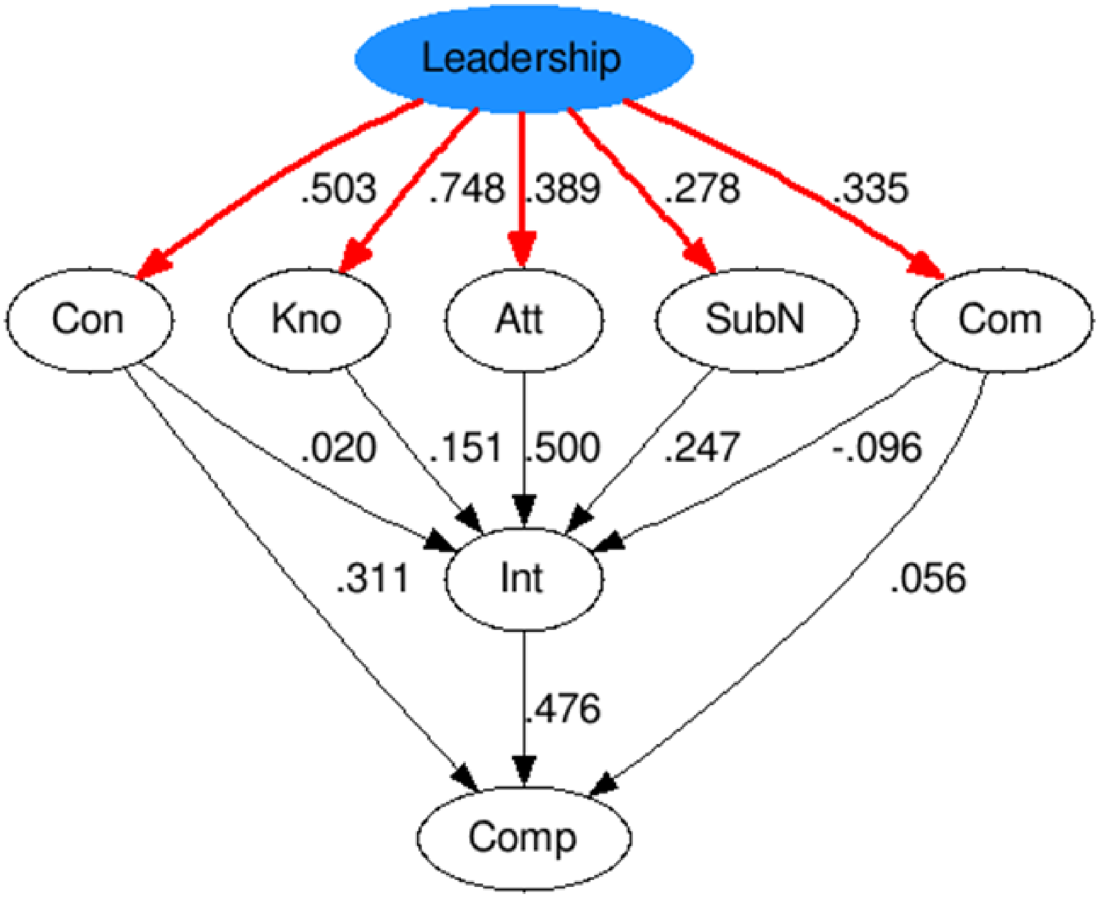

Fig. 2. Structural Path

From our result, we also observed the importance of leadership participation in fostering organisational compliance to cybersecurity control measures and prescriptions. The significant impact of organisational leadership on cultural values and employee cognitive belief is an indication that organisational compliance to cybersecurity has gone beyond delegated responsibility. All the hypothesis linking leadership to all the other variables are strongly supported by our data. (See Fig (2) The effect of knowledge on intention is also significant at Beta = 0.15 at p<0.05 and is consistent with other studies where perceived behavioural control was used as a construct. [42],[19], [31]. Therefore the higher the cognitive ability to understand and apply security controls the more likely the employee will behave in accordance with security principles and practices and this is achieved through establishing a process of regularly educating the employees to sharpen their cognitive understanding on why security controls are necessary, training them on how to apply these controls for the protection of cyber-infrastructure and also creating awareness on their respective roles in the entire security process of the organisation.

It also interesting to note that influence of cybersecurity knowledge on intention as a precursor to compliance is weak when compared to that of rule-oriented cultural value on compliance at Beta = 0.311, further confirming that cognitive understanding of security roles and having practical skills to apply controls according to prescribed procedure does not guarantee compliance if it conflicts with individual beliefs and organisation values [65]. Furthermore, it is noteworthy that the results show that Leadership has a significant influence on cultural values at Beta = 0.503 for (culture of consistency) Controlled cultural value and Beta = 0.344 for Competitive cultural value. The direct effect of cultural value on compliance which is one of our hypothesised relationships is also significant at Beta = 0.296.

Bootstrapping analysis also showed that the indirect effect of Leadership through controlled cultural value is significant at Beta 0.149 while such an effect was very low and insignificant through competitive culture. However, the total indirect effect of leadership on actual compliance which is our outcome target construct is significant at beta 0.350. As suggested by [55] the indirect effect at 97.5 per cent boot confidence interval (Controlled lower limit =.042 and upper limit = 0.296) did not straddle a zero in between indicating that (Culture of consistency) controlled cultural value partially mediates in the influence of leadership on actual compliance.

5.3 Moderating Effect

In order to demonstrate the moderating effect, we extended the model by including the moderator variable; security technology, which we assumed will weaken the relation between intention to comply and actual compliance. We then include the construct; security technologies as our moderating variable and run the PLS algorithm. The evaluation of the moderator variable shows that the constructs measures are reliable and valid. The measurement properties of some of the other constructs also changed slightly. The interaction term has a negative effect on compliance (-0.084), whereas the simple effect of intention to comply on actual compliance is 0.404 (Fig 4). However, if the relationship between the employee intention and actual compliance is reduced by the value of the interacting item ie -0.084, its effect on compliance will increase by the size of the interacting item (0.409-(-0.084), indicating the presence of moderating effect as shown in Fig 5.

The graph on Fig 4 shows that the relationship between intention to comply and actual compliance is positive for all the three-line are indicated by their positive slope. The higher the intention the higher the compliance. In addition, we can see the effect of the moderator variable; security technologies. The green line which represents the high level of the moderator construct has a flatter slope while the blue line which represents the lower level of moderator construct has a steeper slope. This makes sense since the interacting effect is negative. However, bootstrapping analysis indicates that the interacting effect of security technology on compliance is not found to be statistically significant. Hence our hypothesis 7 is not supported by our data.

6 DISCUSSION

Our first main objective was to develop a multi-theory model that better increased our understanding of how organisational cultural values impact on employee security behaviour. The second main objective was to examine which of the theoretical component plays a significant role in fostering organisational cybersecurity compliance and finally to investigate the role of security technology in moderating behavioural compliance with cybersecurity policy. By integrating relevant components of different theories; the theory of planned behaviour, competing value framework and technology organisation environment theory, the research proposed and validated a multi-theory research model designed to increase our understanding of organisational cybersecurity management.

We are able to show that knowledge, attitude, subjective norms significantly and positively impacted the employee's intention to comply with cybersecurity policy requirements. We are also able to show the significant and positive influence of organisational leadership on cultural values and employees cognitive beliefs about organisational cybersecurity.,

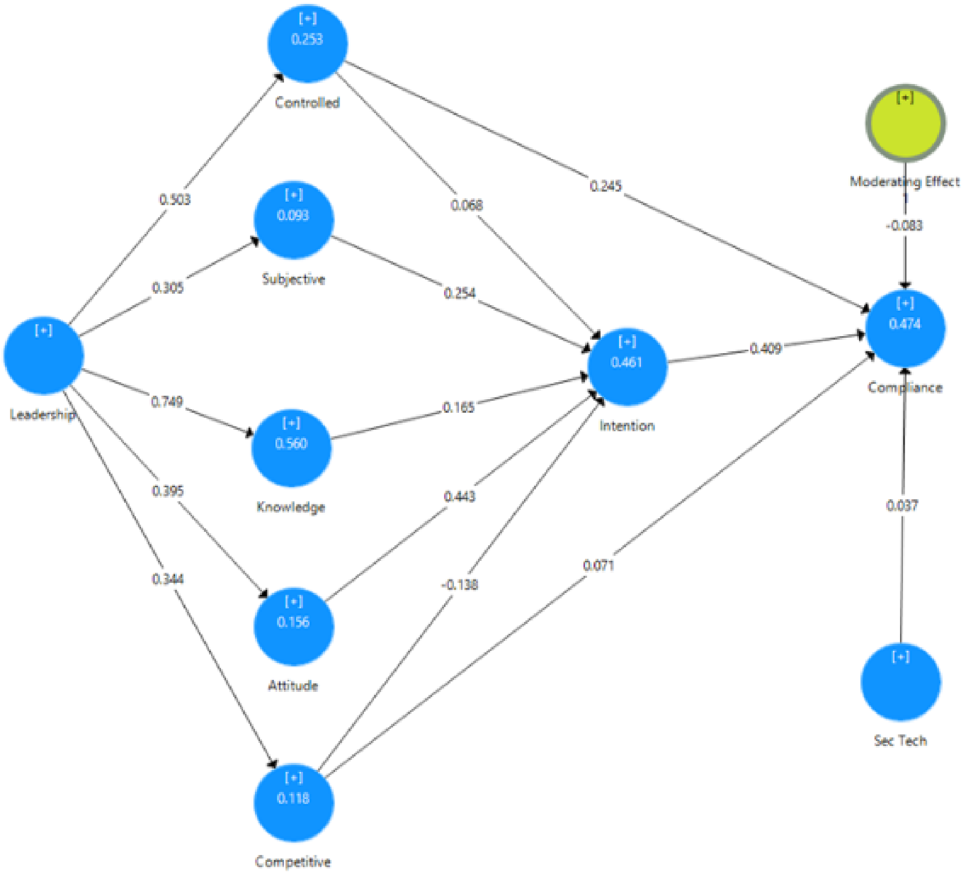

Fig. 3. Moderating Variable

thereby explicating the importance of the involvement of leadership through institutionalising security process and the necessary structure which will enhance the development and application of cognitive understanding in cybersecurity management.

The research also shows that intention to comply with organisation cybersecurity policy requirements has a high and positive influence on actual compliance to security policy requirements. Surprisingly, the result of our research did not support the hypothesised positive relationship between controlled and competitive cultural values on employees intention to comply with organisational cybersecurity requirement, an indication that cultural values do not have a direct impact on employees behavioural intentions. This result is consistent with the empirical findings of [27]. The significant and positive influence of controlled cultural value (culture of consistency) and the insignificant and weak impact of competitive cultural value on compliance is worthy of mention. This kind of opposing relationships could be explained in view of our research context which is more of a bureaucratic environment where the cultural value of rule orientation is extolled. High-Level compliance is expected in such an organisation if leadership incorporates cybersecurity as a strategic tool for achieving the organisational goal by aligning cybersecurity proscribed procedures and control measures with other organisational objectives to increase employee's belief on the value of compliance.

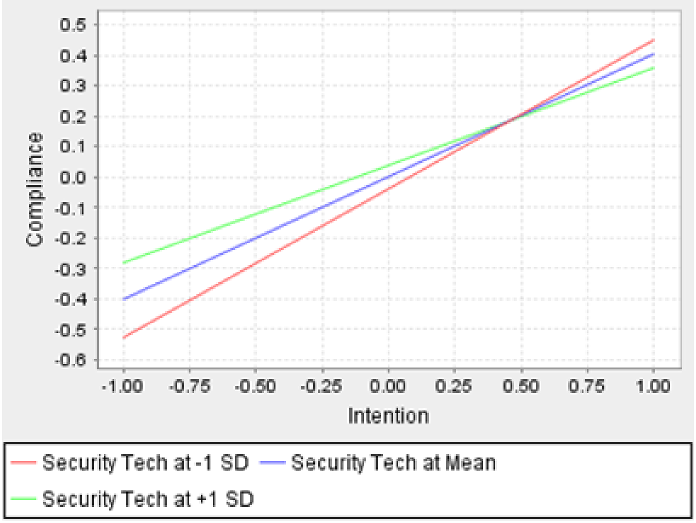

Fig. 4. Moderating Effect

The result also shows that the influence of organisational leadership on employee security behaviour is mediated by cultural values. Confirming one of the main objectives of our study which is to increase our understanding of how organisational cultural values measured by OCAI influences compliance to cybersecurity control measure and prescribed procedures. We also note that the positive significant influence of organisational leadership on cultural values (LEA Beta = .504 and Beta =.344 at P<0.05) and also that of cultural values on organisational compliance to security procedure (Con Beta = 0.296).

Using bootstrapping analysis to examine the indirect effect according to [55] further indicated that cultural values explained part of the influence the leadership has on employee security behaviours. Therefore for a lasting and sustainable compliant behaviour, the organisational leadership must take into consideration the prevailing cultural value in developing, implementing and training employees on organisational cybersecurity process and protocols.

We also observed from our result that the effect of moderating variable is not statistically significant even where the model predictive power was influenced by 1.2 per cent. This is however surprising because other streams of research have demonstrated the usefulness of security technologies is facilitating compliance [19],[28].

Security technology is known to constrain employee to behave in a particular way in response to compliance or noncompliance to organisational cybersecurity requirement. The only explanation we could offer for this is perhaps due to the research environment which is purely a bureaucratic and technologically enabled, hence as a manifest organisational value, leadership incorporates security principles and practices in organisational processes and routines.

6.1 Total Effect

One of the unique features of SmartPls is the ability to assess the direct and indirect effect of non-hypothesised relationships. Though the direct relationship between cybersecurity knowledge as a control belief element and compliance was not hypothesised in our model, however, its total influence on behavioural compliance which is the most important outcome variable in our research is predicted as presented in the total influence table (5). From the postulations of TPB, the actual behaviour of interest is jointly determined by both locus of control and attitude. We, therefore, assumed that in the context of security compliance, when an individual form intentions they take into account how much knowledge they have (locus of control) to enable them to have control over the security behavioural practice of interest. This joint determination of behaviour can be understood in two ways; the first relates to motivation; an individual who has the cybersecurity knowledge and has formed the intention to perform a behaviour of interest will simply try harder. The second is that the failure of an individual to act on his/her intention could be attributable to the lack of adequate cybersecurity knowledge. In this case, it is apparently the absence of cognitive ability and practical skill to rightly apply the security control measures were responsible for the failure to act on the intention. From our research, cybersecurity knowledge came out as one of the top influencers of security behavioural compliance with a total influence factor of 0.307 which is significant at p = 0.05. Hence going by its weak significant relationship of = 0.151 with intention to comply, and a moderate direct effect of 0.245 on compliance, we can reasonably conclude that; to the extent that the knowledge of cybersecurity security is accurate in reflecting the actual determinants of security control measures, a measure of cybersecurity knowledge should help to predict the actual security behavioural compliance which supports the argument of [26] on the influence of PBC on actual behaviour.

Table 5. Total Effect

Construct	Total Effect
Intention>>Compliance	0.476
Leadership>>Compliance	0.344
Con-Culture>>Compliance	0.321
Knowledge>>Compliance	0.307
Attitude>>Compliance	0.238
Sub-Norm>>Compliance	0.118
Comp-culture>>Compliance	0..011

Knowledge of cybersecurity as a control behavioural component, therefore, could only help to predict actual security compliance behaviour if the individual has sufficient experience with the security behaviour of interest to be able to make a reasonable and accurate estimate of his or her control over the behaviour.

6.2 Implication of Research

The study offers important theoretical contributions to researchers in cybersecurity and behavioural sciences. First, this research proposes and validates research conceptualisation that integrates three major theoretical frameworks about individual behaviour, the organisational element of leadership, organisational culture, into one theoretical model. The fusion of the various theoretical frameworks permits a better understanding of the role of various organisational and behavioural mechanisms in fostering organisational cybersecurity compliance. Researchers in behavioural sciences may, therefore, wish to consider integrating various theoretical perspectives from differing domains as was the case of [20], [35],[69], as such approach serves to deepen our understanding in the area.

Secondly, our result did not only support mainstream literature in information security but also lays credence to the resilience of the theory of planned behaviour in the development of individual cognitive processes and predicting the behaviour of interest. In complementing the extant literature, the study further extends the call for attention to how the interaction of organisational factors, behavioural mechanism, and technological environment influence cognitive belief and compliance.

Thirdly, this current study broadens our knowledge on the complementary role of leadership and organisational culture is fostering cybersecurity compliance. For instance the involvement of leadership in structuring cybersecurity processes and programmes and the incorporation of security objectives in work processes and organisational routines through the establishment of structures for support and monitoring, increases employees belief on the value of compliance. Hence the rule orientation cultural value provides the supporting framework for the realisation of the organisational cybersecurity goal.

Achieving organisational compliance to cybersecurity, therefore, requires leadership to re-enforce the behavioural control security mechanisms by encouraging initiatives which send strong legitimacy to and increases employee's value for such a mechanism of control. Such value integration has become necessary for enhancing insight into further theory development as cybersecurity is fast becoming a strategic tool for achieving organisational efficiency and effectiveness[17]

7 CONCLUSIONS, LIMITATIONS, AND FUTURE WORKS

The research suggests that leadership is responsible for the development of employee cognitive mechanisms for the understanding of their security roles and skill necessary for the right application of security controls. The organisation can increase their compliance success rate by establishing processes and structure that conspires with employee cognitive development at the same offering incentives for employees ingenuity in creatively applying security controls in managing, mitigating and minimizing the impact of security breaches.

In view of the influence of leadership on employees attitude, maintaining regular interaction with the employee will improve compliance success through reinforcement of organisational values. This can be achieved through regular in-house orientations, visible display of cybersecurity artefacts and regular communication of organisational security tips specifically designed to accommodate employee's value orientation.

Since cybersecurity has progressively become a tool for competitive advantage and a strategy for achievement of organisational goals, the study, therefore, is of the opinion that active involvement of organisation leadership does not only influence cultural values but also the employee's cognitive belief mechanisms are equally challenged towards positive compliance behaviour. The study, further, suggests the development of an organisational culture where cybersecurity processes and procedures are well defined, employees cybersecurity job roles and descriptions are well articulated, integrated and coordinated by the leadership. A resounding success in organisational compliance with cybersecurity policies and procedures are achieved when all these qualities are evaluated based on strict compliance with rules.

Additionally, the findings of the research suggest that managers need to integrate the process and structure for organisational cognitive and skill development in line with employee job role while creative application of cybersecurity skills in defence of organisation information technology assets should be rewarded to enhance compliance behaviour. Cybersecurity education, training, and awareness should, therefore, be targeted towards clarifying employee's role in the organisation security process, developing competence and practical skill for application of control through cybersecurity security certifications and creatively adapting the various security knowledge in the management of the organisational security network.

Obviously, our study is not without limitations. First, the research was only conducted in three key public sector information technology organisations representing the policy, infrastructure and service sector in Nigeria. Though common method biased was not a problem in this research, however, we do not rule out the possibility of that participant provided socially desirable responses. Our sample is 122, though enough to satisfy the requirement to run a PLS technique, however, the result should be taken with caution as we opined that a larger sample may have yielded a more statistical power and performance. Another major limitation of our work is the multidimensional and complex concept of organisational culture. Selecting a particular dimension, frameworks or cultural values over the other imposes limitation as to what is included.

Future work in this area may consider using other organisational cultural framework or dimension and in a different context. It will also be of importance to know why the moderating effect of security technologies is not significant especially where there ample researches that have linked technological artefacts to employee security behaviour[19], [28]. For instance, we may want to know how the presence of security technologies such as public key infrastructure and digital certificate facilitates employee's compliance with organisational security requirement and control.

ACKNOWLEDGMENTS

The authors would like to thank the National Information Technology Development Agency, Nigeria for sponsoring this programme.

REFERENCES

[1] Icek Ajzen. 2005. *Attitudes, personality, and behavior.* McGraw-Hill Education (UK).

[2] Bernard M Bass and Bruce J Avolio. 1990. Developing transformational leadership: 1992 and beyond. *Journal of European industrial training* (1990).

[3] Daniel Bell. 1999. The axial age of technology foreword: 1999. *The coming of the post-industrial society* (1999), ix–lxxxv.

[4] Rebecca Bryant. 2001. What kind of space is cyberspace. *Minerva-An Internet Journal of Philosophy* 5, 2001 (2001), 138–1.

[5] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly* 34, 3 (2010), 523–548.

[6] Edward G Carmines and Richard A Zeller. 1979. *Reliability and validity assessment.* Vol. 17. Sage publications.

[7] Shuchih Ernest Chang and Chin-Shien Lin. 2007. Exploring organizational culture for information security management. *Industrial management & data systems* (2007).

[8] William R Claycomb, Carly L Huth, Lori Flynn, David M McIntire, Todd B Lewellen, and CERT Insider Threat Center. 2012. Chronological Examination of Insider Threat Sabotage: Preliminary Observations. *J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.* 3, 4 (2012), 4–20.

[9] Sheldon Cohen. 1988. Perceived stress in a probability sample of the United States. (1988).

[10] Lena Yuryna Connolly, Michael Lang, John Gathegi, and Doug J Tygar. 2017. Organisational culture, procedural countermeasures, and employee security behaviour. *Information & Computer Security* (2017).

[11] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. Future directions for behavioral information security research. *computers & security* 32 (2013), 90–101.

[12] Critical Infrastructure Cybersecurity. 2014. Framework for Improving Critical Infrastructure Cybersecurity. *Framework* 1, 11 (2014).

[13] Adéle Da Veiga. 2016. A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. In *2016 SAI Computing Conference (SAI).* IEEE, 1006–1015.

[14] Adéle Da Veiga and Jan HP Eloff. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29, 2 (2010), 196–207.

[15] John D'Arcy, Anat Hovav, and Dennis Galletta. 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research* 20, 1 (2009), 79–98.

[16] Thomas H Davenport, Laurence Prusak, et al. 1998. *Working knowledge: How organizations manage what they know.* Harvard Business Press.

[17] Ronald J Deibert and Rafal Rohozinski. 2010. Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology* 4, 1 (2010), 15–32.

[18] Rocco Depietro, Edith Wiarda, and Mitchell Fleischer. 1990. The context for change: Organization, technology and environment. *The processes of technological innovation* 199, 0 (1990), 151–175.

[19] Tamara Dinev and Qing Hu. 2007. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems* 8, 7 (2007), 23.

[20] Waldo Rocha Flores, Egil Antonsen, and Mathias Ekstedt. 2014. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security* 43 (2014), 90–110.

[21] Claes Fornell and David F Larcker. 1981. Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research* 18, 1 (1981), 39–50.

[22] Bill Gates. 1999. Business@ the speed of thought. *Business Strategy Review* 10, 2 (1999), 11–18.

[23] Asghar Ghasemi and Saleh Zahediasl. 2012. Normality tests for statistical analysis: a guide for non-statisticians. *International journal of endocrinology and metabolism* 10, 2 (2012), 486.

[24] Rebecca A Grier. 2012. Military cognitive readiness at the operational and strategic levels: A theoretical model for measurement development. *Journal of Cognitive Engineering and Decision Making* 6, 4 (2012), 358–392.

[25] Nadine Guhr, Benedikt Lebek, and Michael H Breitner. 2019. The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory. *Information Systems Journal* 29, 2 (2019), 340–362.

[26] Joshua J Guyer and Leandre R Fabrigar. 2015. Attitudes and behavior. (2015).

[27] Joe F Hair Jr, Marko Sarstedt, Lucas Hopkins, and Volker G Kuppelwieser. 2014. Partial least squares structural equation modeling (PLS-SEM). *European business review* (2014).

[28] Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur, and H Raghav Rao. 2014. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information systems journal* 24, 1 (2014), 61–84.

[29] Tejaswini Herath and H Raghav Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47, 2 (2009), 154–165.

[30] Dirk Hovorka and Kai Larsen. 2017. Modes of theory integration. In *Proceedings of the 50th Hawaii International Conference on System Sciences.*

[31] Qing Hu, 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* 43, 4 (2012), 615–660.

[32] John Hulland. 1999. Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic management journal* 20, 2 (1999), 195–204.

[33] Norshima Humaidi and Vimala Balakrishnan. 2013. Exploratory factor analysis of user's compliance behaviour towards health information system's security. *Journal of Health & Medical Informatics* 4, 2 (2013), 2–9.

[34] Norshima Humaidi and Vimala Balakrishnan. 2018. Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal* 47, 1 (2018), 17–27.

[35] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95.

[36] Alexandros Kaliontzoglou, Panagiotis Sklavos, Thanos Karantjias, and Despina Polemi. 2005. A secure e-Government platform architecture for small to medium sized public organizations. *Electronic Commerce Research and Applications* 4, 2 (2005), 174–186.

[37] Atreyi Kankanhalli, Hock-Hai Teo, Bernard CY Tan, and Kwok-Kee Wei. 2003. An integrative study of information systems security effectiveness. *International journal of information management* 23, 2 (2003), 139–154.

[38] Weiling Ke and Kwok Kee Wei. 2008. Organizational culture and leadership in ERP implementation. *Decision support systems* 45, 2 (2008), 208–218.

[39] Bilal Khan, Khaled S Alghathbar, Syed Irfan Nabi, and Muhammad Khurram Khan. 2011. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management* 5, 26 (2011), 10862–10868.

[40] Ned Kock. 2009. Information systems theorizing based on evolutionary psychology: an interdisciplinary review and theory integration framework. *Mis Quarterly* (2009), 395–418.

[41] Ned Kock and Pierre Hadaya. 2018. Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal* 28, 1 (2018), 227–261.

[42] Hennie A Kruger and Wayne D Kearney. 2006. A prototype for assessing information security awareness. *Computers & security* 25, 4 (2006), 289–296.

[43] Dorothy E Leidner and Timothy Kayworth. 2006. A review of culture in information systems research: Toward a theory of information technology culture conflict. *MIS quarterly* 30, 2 (2006), 357–399.

[44] Moez Limayem, Sabine Gabriele Hirt, and Christy MK Cheung. 2007. How habit limits the predictive power of intention: The case of information systems continuance. *MIS quarterly* (2007), 705–737.

[45] Eric Luiijf, Kim Besseling, and Patrick De Graaf. 2013. Nineteen national cyber security strategies. *International Journal of Critical Infrastructures 6* 9, 1-2 (2013), 3–31.

[46] Olive Lundy. 1994. From personnel management to strategic human resource management. *International Journal of Human Resource Management* 5, 3 (1994), 687–720.

[47] Andy Luse, Julie A Rursch, and Doug Jacobson. 2014. Utilizing structural equation modeling and social cognitive career theory to identify factors in choice of IT as a major. *ACM Transactions on Computing Education (TOCE)* 14, 3 (2014), 1–19.

[48] Emily Matta. 2018. Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage. *U. Kan. L. Rev.* 67 (2018), 823.

[49] David C McClelland and Richard E Boyatzis. 1982. Leadership motive pattern and long-term success in management. *Journal of Applied psychology* 67, 6 (1982), 737.

[50] SP NIST. 1998. 800-16 (1998). *National Institute of Standards and Technology (NIST) information technology training requirements: A role-and performance-based model (NIST Special Publication 800-16). Washington, DC: US Department of Commerce* (1998).

[51] Ikujiro Nonaka and Hirotaka Takeuchi. 1995. *The knowledge-creating company: How Japanese companies create the dynamics of innovation.* Oxford university press.

[52] Peter G Northouse. 2019. *Introduction to leadership: Concepts and practice.* SAGE Publications, Incorporated.

[53] Aristotle Onumo, Andrea Cullen, and Irfan Ullah-Awan. 2017. An empirical study of cultural dimensions and cybersecurity development. In *2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud).* IEEE, 70–76.

[54] Kathryn Marie Parsons, Elise Young, Marcus Antanas Butavicius, Agata McCormac, Malcolm Robert Pattinson, and Cate Jerram. 2015. The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making* 9, 2 (2015), 117–129.

[55] Kristopher J Preacher and Andrew F Hayes. 2004. SPSS and SAS procedures for estimating indirect effects in simple mediation models. *Behavior research methods, instruments, & computers* 36, 4 (2004), 717–731.

[56] Petri Puhakainen and Mikko Siponen. 2010. Improving employees' compliance through information systems security training: an action research study. *MIS quarterly* (2010), 757–778.

[57] Robert E Quinn and John Rohrbaugh. 1983. A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. *Management science* 29, 3 (1983), 363–377.

[58] Boumediene Ramdani, Delroy Chevers, and Densil A Williams. 2013. SMEs' adoption of enterprise applications: A technology-organisation-environment model. *Journal of Small Business and Enterprise Development* 20, 4 (2013), 735–753.

[59] Alfonso Reyes and Roberto Zarama. 1998. The process of embodying distinctions—A re-construction of the process of learning. *Cybernetics & Human Knowing* 5, 3 (1998), 19–33.

[60] Christian M Ringle, Sven Wende, Jan-Michael Becker, et al. 2015. SmartPLS 3. *Boenningstedt: SmartPLS GmbH* (2015).

[61] Stephen P Robbins. 2009. *organisational behaviour in Southern Africa.* Pearson South Africa.

[62] Nader Sohrabi Safa, Mehdi Sookhak, Rossouw Von Solms, Steven Furnell, Norjihan Abdul Ghani, and Tutut Herawan. 2015. Information security conscious care behaviour formation in organizations. *Computers & Security* 53 (2015), 65–78.

[63] Marko Sarstedt, Christian M Ringle, Jörg Henseler, and Joseph F Hair. 2014. On the emancipation of PLS-SEM: A commentary on Rigdon (2012). *Long range planning* 47, 3 (2014), 154–160.

[64] Edgar H Schein. 2004. *Organizational culture and leadership (Jossey-Bass business & management series).* Jossey Bass Incorporated.

[65] Thomas Schlienger and Stephanie Teufel. 2003. Information security culture-from analysis to change. *South African Computer Journal* 2003, 31 (2003), 46–52.

[66] STANDARDIZATION SECTOR and OF ITU. [n.d.]. ITU-Tx. 1205. *Interfaces* 10, 20-X ([n. d.]), 49.

[67] Albert H Segars and Varun Grover. 1999. Profiles of strategic information systems planning. *Information Systems Research* 10, 3 (1999), 199–232.

[68] Samuel Sanford Shapiro and Martin B Wilk. 1965. An analysis of variance test for normality (complete samples). *Biometrika* 52, 3/4 (1965), 591–611.

[69] Mikko Siponen, M Adam Mahmood, and Seppo Pahnila. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & management* 51, 2 (2014), 217–224.

[70] Mikko Siponen and Anthony Vance. 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly* (2010), 487–502.

[71] Mikko Siponen and Anthony Vance. 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS quarterly* (2010), 487–502.

[72] Diana K Smetters and Rebecca E Grinter. 2002. Moving from the design of usable security technologies to the design of useful secure applications. In *Proceedings of the 2002 workshop on New security paradigms*. 82–89.

[73] Linda Smircich. 1983. Concepts of culture and organizational analysis. *Administrative science quarterly* (1983), 339–358.

[74] Detmar W Straub Jr. 1990. Effective IS security: An empirical study. *Information Systems Research* 1, 3 (1990), 255–276.

[75] Shuhaili Talib, Nathan L Clarke, and Steven M Furnell. 2013. Establishing a personalized information security culture. In *Contemporary Challenges and Solutions for Mobile and Multimedia Technologies*. IGI Global, 53–69.

[76] Michel Tenenhaus, Vincenzo Esposito Vinzi, Yves-Marie Chatelin, and Carlo Lauro. 2005. PLS path modeling. *Computational statistics & data analysis* 48, 1 (2005), 159–205.

[77] Ioanna Topa and Maria Karyda. 2015. Identifying factors that influence employees' security behavior for enhancing ISP compliance. In *International Conference on Trust and Privacy in Digital Business*. Springer, 169–179.

[78] Haridimos Tsoukas and Efi Vladimirou. 2001. What is organizational knowledge? *Journal of management studies* 38, 7 (2001), 973–993.

[79] Tom R Tyler and Steven L Blader. 2005. Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal* 48, 6 (2005), 1143–1158.

[80] Nils Urbach, Frederik Ahlemann, et al. 2010. Structural equation modeling in information systems research using partial least squares. *Journal of Information technology theory and application* 11, 2 (2010), 5–40.

[81] Jaap J Van Muijen. 1999. Organizational culture: The focus questionnaire. *European Journal of work and organizational psychology* 8, 4 (1999), 551–568.

[82] Anthony Vance, Mikko Siponen, and Seppo Pahnila. 2012. Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management* 49, 3-4 (2012), 190–198.

[83] HS Venter and Jan HP Eloff. 2003. A taxonomy for information security technologies. *Computers & Security* 22, 4 (2003), 299–307.

[84] Rossouw Von Solms and Johan Van Niekerk. 2013. From information security to cyber security. *computers & security* 38 (2013), 97–102.

[85] Kenneth A Wallston. 2015. Control beliefs: Health perspectives. (2015).

[86] Fang Zhao, Alan Collier, and Hepu Deng. 2014. A multidimensional and integrative approach to study global digital divide and e-government development. *Information Technology & People* (2014).

Table 6. Survey Items and heir Loadings

Construct	Item	Factor
Subjective Norm	SUB-N1	0.875
	SUB-N2	0.876
	SUB-N3	0.782
	SUB-N4	0.782
Attitude	ATT1	0.889
	ATT2	0.928
	ATT3	0.899
	ATT4	0.529
Intention	INT1	0.762
	INT2	0.770
	INT3	0.795
	INT4	0.856
Compliance	COMP1	0.923
	COMP2	0.888
Controlled Culture	CON1	0.841
	CON2	0.745
	CON3	0.719
	CON4	0.711
	CON5	0.815
	CON6	0.765
Competitive Culture	COM1	0.796
	COM2	0.658
	COM3	0.838
	COM4	0.824
	COM5	0.792
	COM6	0.816
Security Technology	TECH1	0.955
	TECH2	0.849
	TECH3	0.933
	TECH4	0.816
Leadership	LEA1	0.786
	LEA2	0.853
	LEA3	0.833
	LEA4	0.865
Knowledge	KNO1	0.843
	KNO2	0.777
	KNO3	0.731
	KNO6	0.791
	KNO7	0.779
	KNO8	0.812

A SURVEY QUESTIONS

- SUB-N1 My boss thinks that I should follow the organisation's Cybersecurity policies beyond the confines of the office
- SUB-N2 My colleague thinks that I should follow the organisation's Cybersecurity policies beyond the confines of the office
- SUB-N3 My Organisation's IT department pressures me to follow the Cybersecurity policies beyond the confines of the office
- SUB-N4 My subordinate thinks that I should follow the organisation's Cybersecurity policies beyond the confines of the office
- ATT1 Following the organisation's cybersecurity policy is a necessity
- ATT2 Following the cybersecurity policies reduces the risk of security breach
- ATT3 Following the cybersecurity policies is a useful behavioural tool to safeguard my organisational IT assets
- ATT4 I deem it inappropriate to visit obscene websites
- INT1 I am certain I will comply with my organisation's cybersecurity policies and routine beyond the organisational level
- INT2 Following cybersecurity policies is more important than fast racking job completion
- INT3 I am certain that I will not visit a site I adjudged to be inappropriate
- INT4 I am certain to follow my organisation's cybersecurity policy
- COMP1 I am conscious of my organisational cybersecurity policies and will willingly follow it accordingly
- COMP2 I practice recommended security behaviour as much as possible
- TECH1 Encrypting our organisational data protects it from unauthorised access
- TECH2 Security technologies such as public key infrastructure/digital certificates reduces incidence of security violations in my organisation
- TECH3 I believe that the use of our secured internet and intranet portal enhances our credibility and performance
- TECH4 IT usage in my organisation should be regularly monitored and audited
- LEA1 The organisation has a system that always remind me of the importance of complying to Cybersecurity policies and acceptable security behaviour
- LEA2 My organisation has an established procedure to regularly monitor and audit compliance to cybersecurity policies
- LEA3 My organisation has an established structure for the implementation of cybersecurity policies
- LEA4 My organisation has a process that regularly educate and keep me aware of the importance of adhering strictly to cybersecurity policies
- KNO1 I understand with clarity the content of my organisation's cybersecurity policy
- KNO2 The cyber security policy, procedure and guidelines clearly states what is expected of me to safe guard information technology assets
- KNO3 I Know what risk it is to me and my organisation when opening an email from an unknown sender especially one with attachment.
- KNO6 I believe I have the skills set for the implementation of controls to safeguard my organisation IT asset
- KNO7 I can adapt my organisation cybersecurity policy in various areas of IT application
- KNO8 I understand why and where the cybersecurity policies are to be applied