A Conceptual Framework for Exploring the Factors Influencing Information Security Policy Compliance in Emerging Economies

Salah Kabanda(✉) and Seapei Nozimbali Mogoane

Department of Information Systems, University of Cape Town, Private Bag X3, Rondebosch 7701, South Africa
salah.kabanda@uct.ac.za, MGNSEA002@myuct.ac.za

Abstract. Information security is an important aspect of every organisation today, specifically in Sub Saharan African (SSA) countries whose economies are perceived to be a growing home ground for cyber criminals. Whilst studies on information security policies (ISP) have offered understanding as to why threat agents do not comply with ISP; this understanding comes mainly from the developed economies, thereby giving a generalised view of ISP compliance. This study identifies the factors influencing ISP compliance within emerging economies of SSA. Following a literature review synthesis of the information security terrain, the findings show that ISP compliance is influenced by three main factors of individual characteristics, organisational and environment characteristics. Further, the findings show how the lack of institutional structures that require organisation to abide to both normative and cohesive pressure; influences organisations not to seek information security legitimacy This then influences how threat agents respond to ISP compliance. The implications of these findings for practice and policy are highlighted.

Keywords: Information security · Information security policy (ISP) · Emerging economies

1 Introduction

Organizations today are making security one of their top priorities and are putting security mechanism in place to protect their organisation. One of these mechanisms is the use of an Information Security Policy (ISP) – a set of guidelines set forth to influence actions and decisions where information security in concerned [1] and in so doing, hope to perpetuate an information security culture. An ISP, outlines roles and responsibilities and expected or acceptable conduct relating to protection of information and is regarded as the foundational and critical element of an information security program [2]. Despite the existence of and importance of an ISP, security related breaches remain, with most emanating from within the organisation, usually from employees who fail to comply with ISP guidelines. These employees are seen as a threat to the organisation (insider threats)

Y. H. Sheikh et al. (Eds.): AFRICOMM 2021, LNICST 443, pp. 203–218, 2022.
https://doi.org/10.1007/978-3-031-06374-9_13

because they have privileges to access critical and sensitive information assets and can communicate and transmit information both internally and externally through electronic connections, puts the organisation at risk. Employees can enact actions that puts institutional data, processes, procedures, assets, and resources at risk [3] resulting in huge financial losses, reputational damage, and at times loss of lives [4]. Addressing noncompliance to ISP, is therefore an important objective of any organization since investment in continuous security compliance behavior has the potential to lead to reduced levels of insider threats [2, 5].

This study examines the phenomenon of ISP in emerging economies on the African continent whose information security landscape is perceived to be a growing home ground for cyber criminals due to, among other factors, the increasing technology usage and novice users [6, 7]. According to Van Niekerk [8], organisation have information security plans in place, however these plans are not often reviewed, updated, and monitored to address potential threats, including insider related. In addition, the factors influencing noncompliance to ISP have not been well understood – with many studies being done in a piecemeal manner, either focusing on psychological aspects of the insider (employee) to understand what leads them to noncompliance behavior; or on management related factors, examining whether the organisation has a conducive environment set to discourage noncompliance; or on technical features of the organisation, to determine their technical readiness to implement an ISP. A comprehensive look at contextual factors influencing compliance is therefore of paramount importance, to develop context specific solutions. There have been minimal studies that examines ISP compliance in Sub Saharan Africa, and this is part of the challenge. The fewer studies on this phenomenon in such contextual environments - perceived to have limited resources to combat security related breaches – translates to lack of understanding to practitioners and policy makers who need to be prepared to address the associated challenges of noncompliance. On this note, the purpose of this study is to identify the factors influencing ISP compliance in emerging economies, and more specifically from the Sub-Saharan Africa context.

2 Related Work

There remains no formal definition of what constitutes an insider threat although most scholar do agree that it emanates from potential threat agents (authorized users and trusted business partners) that have legitimate access to sensitive/confidential material, and they may know the vulnerabilities of the deployed systems and business processes in the organisation [9, 10]. Threat actions of potential agents, either intentionally or unintentionally compromise the organisation, causing a significant security concern for academia and practitioners due to the growing number of malicious insider incidents [11]. Several studies have examined this phenomenon with the purpose of understanding what triggers insider threats to occur. A general understanding shows that the organization's practices and managerial processes may create a working environment conducive to insider threats [10]. This understanding, however, has not been contextualized to organisation situated in emerging countries whose organisation practices and managerial processes are yet to be empirically investigated to showcase how they contribute towards an environment conducive to insider threats. The challenge is further compounded by the

availability of insider threat models that detect malicious insiders – however these models have not been tested empirically [12]. The few studies that have examined organisation practices or managerial processes show that these organizations do not see security as a priority, and even if they do, they are faced with organisation or environmental challenges associated with achieving a secure environment [13]. For example, Dagada and Mukwevho [14] explain that the widespread presence of industrial espionage in South Africa could be an indicator that firms do not have adequate security frameworks in place to protect themselves.

In most cases, these organisations have not reflected on their own practices and have not paid attention to the insider threat agent – specifically on the factors that would influence the agent to act in a manner that would cause a threat to the organisation. Paying attention to the insider threat agent in emerging countries is important given the different contextual differences with the developed economies. This study focuses on a type of threat – information security threat which compromises information confidentiality, integrity and its availability [15]. Our focus on information security is deliberate and is motivated by van Niekerk' study [8] showing that out of the 54 cyber-incidents that affected South Africa, the most common impact type was data exposure, which was seen to be caused by accidental/misconfiguration as shown by the "e-billing portal of mobile operator MTN was found to be providing users with access to bills of other customers, and the website was taken offline to correct the error". Another observation was the increase in hacktivism potentially linked to increased political tensions in the country – as seen by the 54% of the cyber-incidents targeted state-owned or political entities as victims.

To address this threat, organisations are advised to implement an information security policy. Yet, compliance is proving to be a challenge, partly because the factors influencing compliance in developing countries are yet to be established due to limited empirical findings; and, because few organisations have implemented such a policy to be able to understand noncompliance. Using literature on the phenomenon specifically that from developing countries in Africa, this study develops a conceptual framework as a steppingstone for future studies that intend to examine insider threat within such contexts.

3 Methodology

A systematic literature review approach was adopted for the study. The first task was to identify the main databases from which the search would be conducted. Given that information security is a multidisciplinary area, the search engines for the study were: ACM Digital Library, IEEE Explore, Scopus and Web of Science. To be specific towards emerging economies and more specifically in Sub Saharan Africa, we included the top ranked IS journals in developing countries according to: Information Technology for Development, Information Technologies and International Development, Electronic Journal of IS in Developing Countries, African Journal of Information and Communication and African Journal of Information Systems. In addition, Google Scholar was used to assist with a broader search of literature for snowballing effect and this added further papers from, for example the African Journal of Science, Technology, Innovation and Development.

A combination of three groups of keywords were used for the search: (1) "Information security", "Information security policy" and synonyms for these terms; (2) "policy compliance"; and (3) "Insider threats" and similar search terms were used. Then, all articles from the search underwent a selection criterion determined on how best the article title, abstract and body addressed the concept of insider threats and information security compliance. Finally, the articles that remained were subjected to thematic synthesis to derive the main key patterns across the data corpus. This process led to three key themes of Individual factors influencing ISP compliance: organizational factors and Environmental factors influencing ISP compliance as shown in Fig. 1. The findings are presented in the next section.

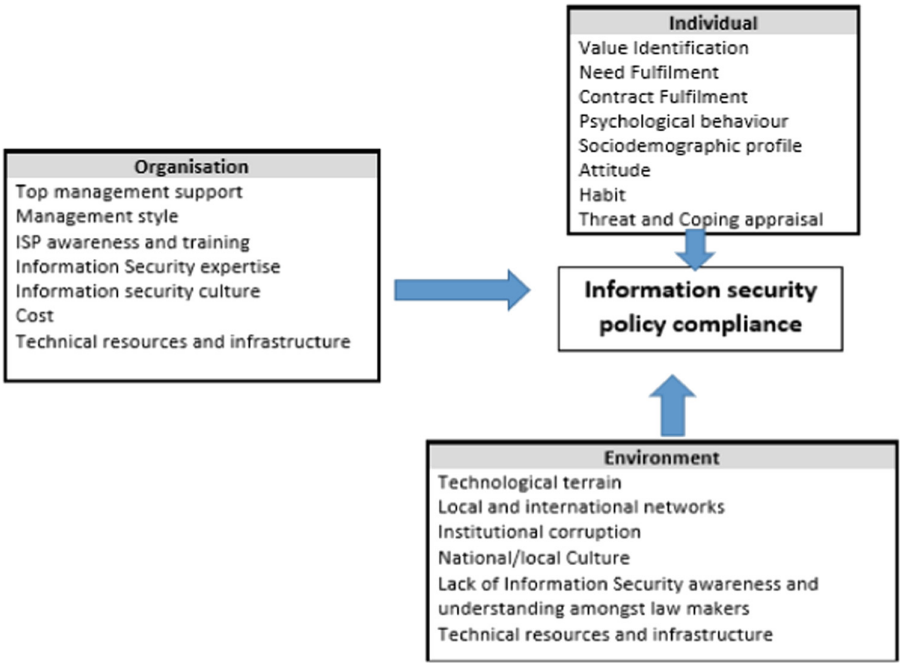

Fig. 1. Conceptual framework

4 Findings

4.1 Individual Factors Influencing ISP Compliance

Psychological Behavior. Most studies have identified humans being as the main cause of security weaknesses and flaws in information systems (IS) and are therefore the critical threat to an organisation's information security. Past studies have therefore decided to focus on the psychological state of the human with the purpose of identifying specific behavioral risk elements. These behavioral risks are then taken as early signs of insider

threats as the individual is more likely to violate security protocols [16]. These behaviors, which emanate from the psychological state of the employee, are brought upon by external and internal factors within the personal life of the employee and tend not to be related to employment.

Need Fulfilment. The importance of need fulfilment is another individual psychological factor requiring consideration. Organisations that have a culture of helping employees fulfil their own self-interests and high order needs for example, self-perceptions of competence, autonomy, and relatedness, recognition and job security, belongingness and love, self-esteem, and self-actualisation [17]; are more likely to have satisfied employees. Such satisfied employees are more likely to comply with information security policies, and therefore exhibit compliance behaviour. Although there are several theoretical lens used to explore the needs fulfilment, the needs theory of motivation in the workplace which "assumes that employees are motivated by more than one need at the same time and can also regress back to lower-level needs as the dominant source of motivation if higher-level needs cannot be fulfilled" [18] is seen as being relevant for studying African countries in the SSA firstly because most are emerging economies and would have compromise different needs; and secondly because insight into how people's needs influence workplaces in SSA's emerging economies are still missing [18]. Therefore, ISP compliance is influenced by the psychological need fulfilment of the threat agent.

Value Identification. One of the psychological factors perceived to influence an individual's behaviour is value identification - the belief in and acceptance of an organisation's mission, vision, and objectives [19]. By identifying with the organisation, employees become willing to "exert considerable efforts on behalf of the organisation in order to achieve a shared goal in the future" [19]. It is therefore proposed that an employee's value identification of the meaning and value of information security influences ISP compliance.

Contract Fulfilment (PCF). Prior studies have tended to approach ISP compliance from a technological deterministic stance. There is now a realisation that such an approach is not enough to address the complexity that arises when an IT solution is used by humans. There is now the addition of psychological contract fulfilment (PCF) – a concept in psychology that explains the exchange relationship between organisations and their employees and "the belief that a promise has been made and a consideration offered in exchange for it, binding the parties to some set of reciprocal obligations" [20]. The challenge with PCF is that they can be interpreted differently by employees [20], and potentially lead to resistance. In-depth studies in PCF show that breach and violation of PCF is a subjective experience that originates from a sense-making process and can be influenced by several factors including culture. This leads to the proposition that PCF influence ISP compliance. This proposition has the potential of explaining why individuals coming from different contextual (socioeconomic, cultural and political) background, would tend to interpret and react to the same PCF differently [20]. Therefore, ISP compliance is influenced by the psychological contract fulfilment of the threat agent.

Sociodemographic Characteristics. Identification of threat agents is important, "as this may help the relevant agents combating the crime in apprehending some of the perpetrators, thereby reducing the incidence" [21]. In the context of emerging countries, various studies have developed a sociodemographic profile of potential threat agents. West Africa in particular, gives a comprehensive account of youths, typically referred to as the yahoo-boys, from the ages of 22–29 years who engage in cybercrime. These youths are said to maintain a distinctive lifestyle of flashy cars, wear expensive and latest clothes and jewelry, prominent at night parties and speak different coded languages [21, 22]. They also have "high technical knowledge and active imagination… manipulative and are bold in risk taking while they have no regard for the law" [21, 22]. They have persuasive techniques and a master of storytelling [34]. These characteristics are seen to confer a unique and/or a notorious identity on them in the society [22]. Therefore, ISP compliance is influenced by the sociodemographic characteristics of the threat agent.

Attitude Towards IS Policies. Attitudes are best explained by the theory of reasoned action (TRA) which espouses that behaviors are largely intentional, and these intentions are guided by their attitude towards that behaviour and their subjective norm [35]. Whilst attitudes define 'favorableness of engaging in a specific behavior' [35]; subjective norm is seen as an individual's perception about certain behavior based on their interaction with others [36]. The Theory of planned behavior (TPB) extended TRA to examine individual behaviour by including self-efficacy related measure of perceived behavioral control that has both an indirect effect through behavioral intentions and a direct effect on behaviour [37]. From these studies, it is postulated that the attitudinal and normative variables influence an individual's intention to comply with information security policies.

Habit. Habit is "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" [38]. In IS, both intention and habit are major antecedents of behaviour and they have been used to explain IS usage [38]. Thus, habits of an individual influence their intention to comply with information security policies.

Threat and Coping Appraisal. In a bid to understand employee's intention to comply to security policies scholars have engaged the Protection Motivation Theory (PMT) to predict human behavioural actions by introducing fear influences. PMT is based on two strong components: threat appraisal and coping appraisal. According to the theory employees who are confronted by information security threats (threat appraisal) and are aware that these threats can cause consequences with a destructive impact on the organization (perceived severity), would have greater intention to comply with information security policies than employees that do not have these perceptions [39]. With regards to coping appraisal, PMT premises that employees who perceive they have the capabilities to apply and adhere to information security policies and have a belief that carrying out the coping action will remove the threat at a feasible cost (sanction), would have greater intention to comply with information security policies than employees that do not have these perceptions [39].

4.2 Organizational Factors Influencing ISP Compliance

Top Management Commitment. Several studies have identified top management support for ISP as one of the requirements for compliance. When senior executives see the significance of information security by attending information security related meetings, become involved in information security related decisions and allocate budget and manpower for information security functions; they send powerful message to the rest of the organisation on the significance of ISP compliance [40]. This message is important because management commitment is usually "measured by employees' perception of efforts made by management to attain information security compliance" [41]. Therefore, ISP compliance is influenced by management commitment towards information security.

Management Style. The role of management support in achieving an organisations objective cannot be under estimated. For management support to be effective, there is a need for an appropriate management style that allows leaders to influence and shape organizational practices and behaviour towards a particular vision, such as an information security culture. According to Guhr et al. [42], transformational leaders are capable of directly influencing employees to exhibit compliance behaviour towards information security practices, because such leaders, "consider the individual needs of their subordinates and encourage them to prioritize the collective over the individual interests as a way to achieve the organizational targets and the wellbeing of the group" [43]. Flores and Ekstedt [44] found transformational leadership strongly associated with both perceived information security culture and information security awareness.

While examining the use of power tactics by hospital administrators to gain employee compliance, Pathania and Rasool [45] found reward power as being the most significant and effective power style in achieving employee behavioural compliance. This was then followed by expert power, referent, legitimate powers, and lastly coercive power. In the SSA, there is no definitive leaderships styles, and it is not clear which forms of power tactics influences compliance. For example, whilst Okeke [46] reports that Nigerian SME owner-managers do not follow any specific leadership style, exhibiting more of transactional leadership than transformational; Dzomonda et al. [47] shows that South African SMEs were more inclined towards transformational leadership style. This background indicates that ISP compliance is influenced by the organisation's leadership management style.

ISP Awareness and Training. Organisations have been advised to engage in information security awareness programs such as establishing ongoing Security Education, Training and Awareness (SETA) programs and use internal and external channels to acquire additional information to address insider threat and compliance to ISP [37]. Hwang et al. [48] show that security education, policy, visibility, and managerial security participation are important for producing security awareness, and usually arises from "both explicit and subjective security experiences in the workplace". These non-technical measures should be seen as an important part of an organisation culture through which employees are made aware of expected and acceptable reasonable security behaviors, especially given the fact that "employees are the weakest link in IS security" [48]. Some

managerial potential solutions to this problem, includes facilitating information security knowledge sharing by motivating staff via intrinsic motivations such as ensuring employees find pleasure and satisfaction from work; and extrinsic motivations such as rewarding employees who exhibit compliance behaviour [49] as well as enforcing an accountability trait in individuals by actioning stipulated sanctions when individuals are caught breaching information security policies [41].

Studies that have examined awareness of compliance have focused on the employee such as those by Al-Omari et al. [50] who examines the effects of users' self-learning and awareness of security issues on compliance behaviour using constructs from the theory of planned behaviour. Using the same theory, Bulgurcu et al. [51] identifies the antecedents of employee compliance with the information security policy (ISP) of an organization and the impact of information security awareness (ISA) on outcome beliefs and an employee's attitude toward compliance with the ISP. Additional studies such as Cheng et al. [52] have used the social bond theory and the general deterrence theory to improve employees' information security behaviour, with the premise their "employees with a stronger bond to their organization are less likely to deviate from policies and participate in delinquent behaviour" [49]. These findings show that awareness and knowledge sharing, collaboration, intervention and experience [49], managerial participation and commitment [48], accountability, as well as "sufficient knowledge, and access to resources (e.g. magazines, discussion forum, and online help) about security issues" can influence attitude toward compliance [50].

Information Security Expertise. The lack of readily available and affordable information security expertise has been highlighted as one of the challenges associated with combating IT related security crimes and can affect an organization's performance and sustainable competitive [53]. Availability of in-house technical experts with high levels of proficiency and experience in information and network security is important to any organisation because such experts are usually sensitive to potential threat cues, understands information security risks and controls and are in the best position to advice on the development of ISPs [54]. However, for most organisations in emerging economies, there are few information security experts and even if they are available, they are seen to be expensive or operate on a tight financial budget which leads to misapplications and consequently to the risk of IS attacks [55]. The lack of an information security expert leads to a weakly designed ISP that are poorly thought out, incomplete, redundant, and irrelevant [56]. Therefore, ISP compliance is influenced by the availability of an information security expert who can design and implement ISPs that address possible internal and external threats.

Cost. The cost associated with implementation and maintenance of an information security program has traditional been costly for organisations in emerging economies [53]. This is partly because organisations in these contexts tend to be small to medium enterprises who are resource constrained in terms of budget and expertise. They have minimal operating budget that includes technical costs to address IT specific matters such as antivirus that provide protection against viruses and a firewall that protect the network connections; as well as educational cost required to prepare the security education for the employees, hiring an external expert or outside training organizations [57]. Therefore,

ISP compliance is influenced by an organisations ability to have access to financial resources to implement and maintain an ISP program.

Information Security Culture. Organizational culture - a pattern of shared basic assumptions or beliefs that a group holds - is perceived to affect the behaviour of employees [58]. An information security culture channels the behaviour of employees to follow information security and related information processing policies and regulatory requirements [59]. When developing and implementing an information security culture, the organisation should be cognisant of the possibility of several information security subcultures that could be present in the organisation emanating from different individuals' geographical, ethnic or age groups, thereby leading to different assumptions, values, and beliefs about the protection of information [59]. This awareness calls for, in some cases, different methods that depend on the subculture and context when dealing with information security problems [60]. Thus, ISP compliance is influenced by the organisational culture which subsequently influences the information security culture.

Technological Resources. Availability of and access to technological resources, specifically information security technologies, to implement and enforce ISP has been identified as one of the main challenges for most organisation. Technological resources include both internal and external technologies relevant to the firm. Cavusoglu et al. [61] sees information security technologies as the extent to which an organization possesses preventive and detective technical solutions to address vulnerabilities within information technology infrastructure in which critical information assets reside. Yet, most emerging countries do not attach as much importance to information technology security as their counterpart companies in developed economies. For example, In South Africa, De Lange et al. [62] reports that half of the municipalities have no controls designed concerning information security, and therefore the issue of security is not well addressed properly. The lack of readily and relevant technological resources has been associated with the high implementation and maintenance costs which most organisations are not able to afford [53]. Having limited to no readily available technological resources can therefore negatively influence ISP because resources associated with ensuring control measures and compliance are not present.

4.3 Environmental Factors

Technological Terrain of Emerging Economies. Most African emerging economies are now increasing technology users, making them to become a growing home ground for cyber criminals [6]. The increase in the penetration of broadband access and therefore internet access has also turned Africa into a fertile ground for online crime [63]. The absence of cyber protective measures, 'existence of vulnerable systems and lax cybersecurity practices' and the lack of compliance to existing cyber security practices, has made Africa to be seen by cyber criminals as a "safe haven to operate illegally with impunity" [6].

Local and International Networking Among the Perpetrators. Emerging economies are perceived to have a poor security landscape partly due to the organized local and international cybercrime networks working together [21]. These networks, according are deemed important for local threat agents to share knowledge about their target and share skills necessary to commit the crime; and the international threat agents who become useful in "clearing of checks and goods" [21]. For example, when cybercrime takes place, most of the banks used in the crime such as wire transferring of funds, tend to be in US. According to Wilson [64], the average employee doesn't have the time or resources to counterattack the threat agent and therefore easily becomes target. Therefore, having measures in place to avoid contact with the threat agent and their networks; as well as understanding how cybercriminal networks arise and develop could assist in protecting an organisation from information and cyber security related threats [65]. With this understanding, it is evident that threat agents that have local and international networks are less likely to comply to ISP because these agents have access to resources which they can exploit for their criminal behaviours.

Institutional Corruption. Apart from the local and international networks working together, [21] identified corruption of local agents who include but not limited to banks, security agencies, co-fraudsters and, sometimes, families, as the main challenge that perpetuate cybercrime in emerging economies. The authors for example identify bank officials and postal agents as being accomplice by making the clearing of any money realized and clearing goods in exchange for compensation from the perpetrators. Ojedokun and Eraye [22] calls for "a strong alliance" between all stakeholders in addressing cybercrime partly because corruption is embedded in the socio-cultural structures of most developing countries [23]. When corruption is prevalent in a society and becomes embedded as an element of the norms and rules, it affects the practices of the organisation and its legitimacy. The lack of support of an anti-corruption culture, particularly political support legitimises corruption [24]; which then influences how employees carry out their tasks; and consequently, contribute towards employee's noncompliance of ISP because employees can engage in corruptive practices that are seen as "acceptable patterns of behaviour that are supported by society" [24].

Culture: Traditional charms – voodoo. In Nigeria, several authors have identified the use of traditional charms and mystical powers to achieve the desired goals of cyber related crimes [21]. Adesina [25] asserts that some threat agents resort to spiritual means: "like voodoo or juju to hypnotize their victims into doing their bidding and parting with whatever amount of money they request for. They… indulge in occultic ritual practices to enhance their potential to defraud people. It involves employing traditional spiritual means like voodoo or juju in ensuring that the cybercriminal hypnotizes his victims and thereby brighten the swindler's chances of getting his victims hypnotised. Once this is successfully done, the victim is guaranteed to keep remitting money from wherever he or she is in the world".

Although these spiritual means of enhancing their businesses have no scientific basis, the technique is perceived by the threat agents as important in influencing their business outcome [21]. Dheer [26] posits that institutional and cultural factors operating at the macro-level facilitate the identification, creation, and exploitation of opportunities

through starting new ventures. Given that cybercrime is a new venture in some emerging economies of Africa, perpetuated by the availability of ICTs; understanding the role of culture in influencing the threat agent's compliance to ISP is important.

Lack of Lawmakers Who Understand Cyber Related Threats. One of the key challenges affecting organisation's implementation of and enforcement of an ISP, is the lack of human resource expertise, specifically lawmakers and Information security practitioners. Quarshie and Martin-Odoom [27] note that the lack of lawmakers who understand cyber related threats is a problem as this affects their ability to implement legislation that addresses cyber threats at legal, policy and regulation level. This is made more complex due to the "legal inadequacies in various jurisdictions and uneven enforcement" [28]. Lawmakers are powerful external agents to an organisation. Their ability to understand information security and cyber security related threats as well as legislations, can exert pressure on an organisation and influence its institutional practices. For example, by having lawmakers with the right skill set, coerces the organisation into adopting ISP and ensuring compliance to the ISP. Of which failure to comply, can lead to sanctions such as prosecution. By complying, the organisation is likely to engage in practices that make it difficult for threat agents to thrive.

Weak Information and Cyber Security Capacity Building Systems. Educational institutions are recognised as first line of defence because the research conducted, contributes to body of knowledge and has the power to directly influence national policies and strategies [29]. Yet, according to Rowe et al. [30], there is a significant shortage of qualified Information Security Professionals despite the field being one of the best compensating fields. Some of the challenges facing information security education in developing countries particularly in Africa, include the lack of governmental support, inadequate curriculums, limited budgets, knowledge by educators. These challenges are in dire need of address because existing efforts have not fostered cyber capacity building efforts [31]. For example, "the extent to which information security is addressed at undergraduate level is on an ad hoc basis, with isolated attention being paid to a few information security aspects" [32].

5 Discussion

Information security is becoming one of the most important aspect of any organisation's performance and long-term survival. By implementing and maintaining an ISP, an organisation provides an outline and control measures for its employees with respect to security behaviour. In addition to being critical at the organizational level, information security is also important at the national level because of the increasing trend of cyber-attacks which is now changing from small-scale intrusion attempts and financial breaches at organizational level, to more highly organized state-sponsored attacks [33]. The link between the individual and the organisation, as well as the organisation and the existing institutions such as the government cannot therefore be ignored. It is at the national level, where institutions are to provide appropriate institutional and social

support structures, for example policies and regulatory conditions, for the implementation and maintenance of effective information security policies. The availability of these structures may result in a more secure IT environment, and "result in penalties for others because the appraisal of such policies and regulations by the people of a nation is vulnerable to their cultural orientation" [26].

In this study, at national level, we identify factors of organised networks both local and international, institutional corruption, traditional culture and the absence of IT experts and lawmakers with IT security expertise as structural constraints to the successful implementation and maintenance of an ISP. At national level, if leaders are not able to challenge these structures that constrain their actions and choices, they then legitimise their existence. When legitimised, this interplay between structures and the leader, influence the leaders (national decision makers') understandings of IT security issues and consequently the action to take. For example, at national level, the availability of institutions with IT experts and lawmakers with IT security expertise can result in the development and implementation of secure information security practices; and so, such institutions can exert coercive and normative pressures on how organization at micro level behaves with regards to information security. The absence of such institutions imply that organisations do not need to achieve legitimacy to operate, i.e. do not need to comply to formal institutional information security policies, and once this is internalised in time, creates a working environment conducive to insider threats [10]. This becomes further exacerbated in organisations facing internal structural constraints of, for example, no management commitment towards an information security culture, lack of internal information security expertise, lack of financial and technological resources. These types of organisations would face high risk of ISP noncompliance than their counterparts who face both coercive and normative pressures to comply. Noncompliance to ISP is further compounded by employees who constrain organisational structures associated with ISP compliance through their cognitive structures of value identification, needs and contract fulfilment. Employees can also use their sociodemographic characteristics, access to local and international networks, institutional corruption, as well traditional charms, as resources to influence ISP compliance and security policies in general.

6 Conclusion

The purpose of this study was to identify the factors influencing ISP compliance in emerging economies, and more specifically from the Sub-Saharan Africa context. The study followed a literature review synthesis of prior work on the phenomenon. The findings show that ISP compliance is influenced by an employee's sociodemographic profile, how an employee perceives how well their needs, value and contract are fulfilled by the organisation; as well as the employee's psychological state which influences behaviour. From an organisation perspective, factors associated with top management commitment and management style, information security culture, ISP awareness and training, availability of ISP resources and expertise as well as the costs to acquire these resources were deemed important in influencing ISP compliance. Finally, a set of contextual factors that influence ISP compliance were identified: institutional corruption, national culture, lack of institutional understanding of cyber related issues, and availability of local and international networks amongst perpetuators.

These three factors, along with human actions, enable and constrain ISP compliance. This study shows how the lack of institutional structures that require organisations to abide to both normative and cohesive pressure; influences organisations not to seek information security legitimacy This then influences how threat agents respond to ISP compliance. Of note is how threat agents can use their individual cognitive resources, their understanding of institutional structures that affords them illegitimate practices (such as corruption behaviour); to challenge organisational structures of complying with ISP.

These findings have implications for practice and policy development. Firstly, is the realisation that emerging economies have institutional structures that are not conducive for information security policy compliance; and that organisations need to bear in mind that the absence of institutional structures can lead to ISP noncompliance. Organisations should therefore tighten their security and engage in an ongoing information security culture, supported by an awareness and training program, and availability of both technological and financial resources. Second, organisations need to understand expectations of employees and stakeholders and engage in ongoing consultations with the purpose of identifying potential risk areas and behaviours that could lead to ISP noncompliance. This engagement should be cognisant of the fact that everyone is different, and their sociodemographic and subcultural characteristics can potentially influence psychological behaviour.

Whilst the findings provide a better explanation of the factors influencing ISP compliance within emerging economies; the study remains at the conceptual level. Although this is a limitation of the study, it should be noted that studies that engage in the development of a conceptual framework in an area that is yet well understood, are beneficial in providing a foundation for the empirical observations to follow. A current ongoing study seeks to use the conceptual framework to empirically explore these factors in-depth within the context of emerging economies.

References

1. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
2. Glaspie, H.W., Karwowski, W.: Human factors in information security culture: a literature review. In: Nicholson, D. (ed.) Advances in Human Factors in Cybersecurity, pp. 269–280. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-60585-2_25
3. Heneke, D., Ophoff, J., Stander, A.: The threats that insiders pose to critical infrastructure–a South African perspective. In: HAISA, pp. 279–289 (2016)
4. Sarkar, K.R.: Assessing insider threats to information security using technical, behavioural and organisational measures. Inf. Secur. Tech. Rep. **15**(3), 112–133 (2010). https://doi.org/10.1016/j.istr.2010.11.002
5. Agrafiotis, I., Nurse, J.R., Buckley, O., Legg, P., Creese, S., Goldsmith, M.: Identifying attack patterns for insider threat detection. Comput. Fraud Secur. **2015**(7), 9–17 (2015)
6. Kshetri, N.: Cybercrime and cybersecurity in Africa. J. Glob. Inf. Technol. Manag. **22**(2), 77–81 (2019)
7. Ben-David, Y., et al.: Computing security in the developing world: a case for multidisciplinary research. In: NSDR 2011, pp. 1–6 (2011)

8. Van Niekerk, B.: An analysis of cyber-incidents in South Africa. Afr. J. Inf. Commun. **20**, 113–132 (2017)
9. Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., Ochoa, M.: Insight into insiders and it: a survey of insider threat taxonomies, analysis, modeling, and countermeasures. ACM Comput. Surv. (CSUR) **52**(2), 1–40 (2019)
10. Moore, A.P., Cassidy, T.M., Theis, M.C., Bauer, D., Rousseau, D.M., Moore, S.B.: Balancing organizational incentives to counter insider threat. In: 2018 IEEE Security and Privacy Workshops (SPW), pp. 237–246. IEEE, May 2018
11. Haidar, D., Gaber, M.M., Kovalchuk, Y.: Anythreat: an opportunistic knowledge discovery approach to insider threat detection. arXiv preprint arXiv:1812.00257 (2018)
12. Nkosi, L., Tarwireyi, P., Adigun, M.O.: Insider threat detection model for the cloud. In: 2013 Information Security for South Africa, pp. 1–8. IEEE, August 2013
13. Padayachee, K.: An assessment of opportunity-reducing techniques in information security: an insider threat perspective. Decis. Support Syst. **92**, 47–56 (2016)
14. Dagada, R., Mukwevho, S.: Industrial espionage threat in corporate South Africa. In: Society of Digital Information and Wireless Communications Conference (2013)
15. Safa, N.S., Maple, C., Watson, T., Von Solms, R.: Motivation and opportunity based model to reduce information security insider threats in organisations. J. Inf. Secur. Appl. **40**, 247–257 (2018)
16. Fagade, T., Tryfonas, T.: Malicious insider threat detection: a conceptual model. Secur. Prot. Inf. **2017**, 31–44 (2017)
17. Velez, J.A., Ewoldsen, D.R., Hanus, M.D., Song, H., Villarreal, J.A.: Social comparisons and need fulfillment: interpreting video game enjoyment in the context of leaderboards. Commun. Res. Rep. **35**(5), 424–433 (2018)
18. Poetz, K.: Establishing socially responsible workplaces: need perceptions and institutional forces acting on MSE owners in Tanzania. Can. J. Adm. Sci./Revue Canadienne des Sciences de l'Administration **33**(3), 197–212 (2016)
19. Li, Y., Zhang, N., Siponen, M.: Keeping secure to the end: a long-term perspective to understand employees' consequence-delayed information security violation. Behav. Inf. Technol. **38**(5), 435–453 (2019)
20. Santos Cesário, F., José Chambel, M., Guillén, C.: What if expatriates decide to leave? The mediation effect of the psychological contract fulfilment. Manag. Res.: J. Iberoamerican Acad. Manag. **12**(2), 103–122 (2014)
21. Aransiola, J.O., Asindemade, S.O.: Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyberpsychol. Behav. Soc. Netw. **14**(12), 759–763 (2011)
22. Ojedokun, U.A., Eraye, M.C.: Socioeconomic lifestyles of the yahoo-boys: a study of perceptions of university students in Nigeria. Int. J. Cyber Criminol. **6**(2), 1001 (2012)
23. Uberti, L.J.: Can institutional reforms reduce corruption? Economic theory and patron–client politics in developing countries. Dev. Chang. **47**(2), 317–345 (2016)
24. Pillay, S., Kluvers, R.: An institutional theory perspective on corruption: the case of a developing democracy. Finan. Accountability Manag. **30**(1), 95–119 (2014)
25. Adesina, O.S.: Cybercrime and poverty in Nigeria. Can. Soc. Sci. **13**(4), 19–29 (2017)
26. Dheer, R.J.S.: Cross-national differences in entrepreneurial activity: role of culture and institutional factors. Small Bus. Econ. **48**(4), 813–842 (2016). https://doi.org/10.1007/s11187-016-9816-8
27. Quarshie, H.O., Martin-Odoom, A.: Fighting cybercrime in Africa. Comput. Sci. Eng. **2**(6), 98–100 (2012)
28. Moraski, L.: Cybercrime knows no borders. Infosecurity **8**(2), 20–23 (2011)
29. Hewitt, B., Kruck, S.E.: Incorporating global information security and assurance in I.S. education. J. Inf. Syst. Educ. **24**(1), 11–13 (2013)

30. Rowe, D.C., Lunt, B.M., Ekstrom, J.J.: The role of cyber-security in information technology education. In: SIGTE Conference, p. 113 (2011)
31. Calderaro, A., Craig, A.J.S.: Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. Third World Q. **41**(6), 917–938 (2020). https://doi.org/10.1080/01436597.2020.1729729
32. Futcher, L., Schroder, C., von Solms, R.: Information security education in South Africa. Inf. Manag. Comput. Secur. **18**(5), 366–374 (2010)
33. Shafqat, N., Masood, A.: Comparative analysis of various national cyber security strategies. Int. J. Comput. Sci. Inf. Secur. **14**(1), 129 (2016)
34. Herley, C.: Why do Nigerian scammers say they are from nigeria?. In: WEIS, June 2012
35. Moody, G.D., Siponen, M., Pahnila, S.: Toward a unified model of information security policy compliance. MIS Q. **42**(1), 285–311 (2018)
36. Khan, H.U., AlShare, K.A.: Violators versus non-violators of information security measures in organizations—a study of distinguishing factors. J. Organ. Comput. Electron. Commer. **29**(1), 4–23 (2019)
37. Bauer, S., Bernroider, E.W.: From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. ACM SIGMIS Database: DATABASE Adv. Inf. Syst. **48**(3), 44–68 (2017)
38. Hsiao, C.H., Chang, J.J., Tang, K.Y.: Exploring the influential factors in continuance usage of mobile social apps: satisfaction, habit, and customer value perspectives. Telemat. Inform. **33**(2), 342–355 (2016)
39. Siponen, M., Pahnila, S., Mahmood, A.: Employees' adherence to information security policies: an empirical study. In: Venter, H., Eloff, M., Labuschagne, L., Eloff, J., Solms, R. (eds.) SEC 2007. IIFIP, vol. 232, pp. 133–144. Springer, Boston (2007). https://doi.org/10.1007/978-0-387-72367-9_12
40. Narain Singh, A., Gupta, M.P., Ojha, A.: Identifying factors of "organizational information security management." J. Enterp. Inf. Manag. **27**(5), 644–667 (2014)
41. AlKalbani, A., Deng, H., Kam, B.: Organisational security culture and information security compliance for E-government development: the moderating effect of social pressure. In: PACIS, p. 65, July 2015
42. Guhr, N., Lebek, B., Breitner, M.H.: The impact of leadership on employees' intended information security behaviour: an examination of the full-range leadership theory. Inf. Syst. J. **29**(2), 340–362 (2019)
43. Rodrigues, A.D.O., Ferreira, M.C.: The impact of transactional and transformational leadership style on organizational citizenship behaviors. Psico-USF **20**(3), 493–504 (2015)
44. Flores, W.R., Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. **59**, 26–44 (2016)
45. Pathania, A., Rasool, G.: Investigating power styles and behavioural compliance for effective hospital administration: an application of AHP. Int. J. Health Care Qual. Assur. **32**(6), 958–977 (2019)
46. Okeke, V.I.: Leadership Style and SMEs Sustainability in Nigeria: A Multiple Case Study (2019)
47. Dzomonda, O., Fatoki, O., Oni, O.: The impact of leadership styles on the entrepreneurial orientation of small and medium enterprises in South Africa. J. Econ. Behav. Stud. **9**(2(J)), 104–113 (2017)
48. Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H.: Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. **37**(12), 1049–1092 (2014). https://doi.org/10.1108/MRR-04-2013-0085
49. Safa, N.S., Von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Comput. Secur. **56**, 70–82 (2016)

50. Al-Omari, A., El-Gayar, O., Deokar, A.: Information security policy compliance: the role of information security awareness (2012)
51. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34**(3), 523–548 (2010)
52. Cheng, L., Li, Y., Li, W., Holm, E., Zhai, Q.: Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. Comput. Secur. **39**, 447–459 (2013)
53. Lee, J.K.: Research framework for AIS grand vision of the bright ICT initiative. MIS Q. **39**(2), iii–xii (2015)
54. Dojkovski, S., Lichtenstein, S., Warren, M.: Enabling information security culture: influences and challenges for Australian SMEs. In: Proceedings of the 21st Australasian Conference on Information Systems, ACIS 2010, January 2010
55. Ng, Z.X., Ahmad, A., Maynard, S.B.: Information security management: factors that influence security investments in SMES. In: Australian Information Security Management Conference. Edith Cowan University, Perth, Western Australia, 2nd–4th December 2013 (2013)
56. Flowerday, S.V., Tuyikeze, T.: Information security policy development and implementation: the what, how and who. Comput. Secur. **61**, 169–183 (2016)
57. Kamariza, Y.: Implementation of information security policies in public organizations: top management as a success factor. Dissertation, pp. 13–37 (2017)
58. Tang, M., Li, M., Zhang, T.: The impacts of organizational culture on information security culture: a case study. Inf. Technol. Manag. **17**(2), 179–186 (2015). https://doi.org/10.1007/s10799-015-0252-2
59. Da Veiga, A., Martins, N.: Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. **49**, 162–176 (2015)
60. Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., Bhattacharya, J.: Analyses of issues of information security in Indian context. Transforming Gov.: People Process Policy **8**(3), 374–397 (2014)
61. Cavusoglu, H., Cavusoglu, H., Son, J.Y., Benbasat, I.: Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf. Manag. **52**(4), 385–400 (2015)
62. De Lange, J., Von Solms, R., Gerber, M.: Better information security management in municipalities. In: 2015 IST-Africa Conference, pp. 1–10. IEEE, May 2015
63. Cassim, F.: Addressing the growing spectre of cyber crime in Africa: evaluating measures adopted by South Africa and other regional role players. Comp. Int. Law J. Southern Afr. **44**, 123–138 (2011)
64. Wilson, J.: Scamming the scammers with their own tricks. Comput. Fraud Secur. **2018**(9), 14–16 (2018)
65. Leukfeldt, E.R.: Organised cybercrime and social opportunity structures. A proposal for future research directions. Eur. Rev. Organ. Crime **2**(2), 91–103 (2015)