INVESTIGATING STAFF INFORMATION SECURITY POLICY COMPLIANCE IN ELECTRONIC IDENTITY SYSTEMS –THE GHANAIAN NATIONAL IDENTITY SYSTEM

Salim Awudu and Sotirios Terzis
Department of Computer and Information Sciences, University of Strathclyde, Glasgow, United Kingdom

ABSTRACT

Information Security Policy (ISP) compliance is key in securing organisational data. Although the factors that influence ISP compliance have been extensively studied, the emergence of Electronic Identity Systems (EIS) organisations like the Ghanaian National Identification Authority (NIA), have placed particular emphasis on the trustworthiness, privacy and security requirements. It is necessary to study these factors in this new context to ensure the security of the system. This paper presents the first study in this area. Prior research has shown the importance of staff attitude and motivation in ISP compliance, with motivation related to the perceived intrinsic benefits and extrinsic rewards for compliance. So, this study uses the NIA as a case study to explore the staff attitude towards ISP compliance and their perceived intrinsic and extrinsic rewards for compliance. A questionnaire-based study was conducted using adapted scales from literature. The results show that both experienced and inexperienced NIA staff recognise the necessity, benefits, importance, and usefulness of the ISP, and feel content, satisfied, accomplished, and fulfilled when complying with it. However, although experienced staff perceptions are clear that extrinsic rewards are not motivating compliance in the NIA, the inexperienced staff perceptions are unclear. These findings reinforce the need for clarity in EIS organisations regarding ISP compliance through formally approved policies and awareness training, they also point towards an opportunity to complement sanctions with rewards to motivate their staff.

KEYWORDS

Electronic Identity Systems, Information Security Policy, Information Security Policy Compliance

1. INTRODUCTION

Over the years, several countries have resorted to Electronic Identity Systems (EIS) to enhance the delivery of their services for citizens and residents. These systems collect and manage personal identification information. Despite the economic, social, and political benefits of such systems, their use has raised growing concerns about their security, privacy, and trustworthiness (Handforth and Matthew, 2019).

According to (Flowerday and Tuyikeze, 2016) “one important mechanism for protecting organizations’ assets is the formulation and implementation of an effective Information Security Policy (ISP)”. However, it is not enough for an organization to have an ISP, staff also need to comply with its provisions. According to (Alzahrani et al., 2018) “understanding the factors that influence employees’ compliance with their organisational ISP is one of the fundamental challenges in (cyber) security management”. Unsurprisingly, a lot of research has been devoted to this as a recent survey demonstrates (Ali et al., 2021). The research has explored a variety of factors that influence employee ISP compliance and has identified attitude towards compliance and motivation for compliance, with more focus on sanctions rather than rewards, as important factors.

In this paper we present the first study on attitude towards compliance and perceived intrinsic benefits and extrinsic rewards for ISP compliance in EIS organisations. We focus on benefits and rewards rather than sanction because of the limited attention they have received in the ISP compliance literature. The study explores these factors in the context of the Ghanaian National Identification Authority (NIA), a typical organisation that faces specific challenges that are not uncommon during the introduction of EIS. In addition to its focus on EIS organisations, the study is also novel in that, it explores how staff experience affects these factors, a question

pertinent to the current circumstances of the NIA that has a lot of new and contracted staff joining the organisation recently. More specifically, a questionnaire-based study was conducted to answer the following research questions:

- What are the attitudes of NIA staff towards ISP compliance?
- What are their perceptions of the intrinsic and extrinsic rewards for ISP compliance?
- Does experience affect ISP compliance attitudes and reward perceptions of NIA staff?

The study built on the measures developed in (Bulgurcu et al, 2010) by focusing on intrinsic benefits and extrinsic rewards for ISP compliance. The results show that NIA staff recognise the necessity, benefits, importance, and usefulness of the ISP, and feel content, satisfied, accomplished and fulfilled when complying with it. This is the case for both experienced and inexperienced staff. However, although experienced staff perceptions are clear that extrinsic rewards are not used to motivate compliance, inexperienced staff are unclear about it. These findings further reinforce the need for clarity in EIS organisations in the form of formally approved policies and awareness training, both areas currently lacking in the NIA. Moreover, they highlight an opportunity in complimenting sanctions with rewards to further motivate staff.

This paper begins with literature review on EIS and ISP compliance in 2, followed by a description of our methodology in 3, presentation of our analysis and findings in 4, a discussion on the implications of our findings in 5, and closing with conclusion and directions for future work in 6.

2. LITERATURE REVIEW

EIS are "system[s] that involve the collection of information or attributes associated with a specific entity" (Wladawsky-Berger, 2016). Several countries, including Ghana, have fully operationalized EIS to collect such information for the purpose of providing services to people within their territory and beyond. Despite the potentially benefits of EIS, concerns have emerged about their potential negative effects, e.g. "once cards are mandatory, then they may be used to single out or even to harass visible minorities and those with alternative lifestyles" (Lyon and Bennett, 2013), or more importantly concerns about the Privacy, Trustworthiness, and Security of the data they collect, store and manage (Raggad, 2010).

To prevent security incidents organizations must have an ISP that reflects local information security philosophy and commitments (Johnson, 2006). More specifically, an ISP is a set of rules or requirements that are related to information security and enacted by an organization to be adhered to by all, to protect the confidentiality, integrity and availability of information and other valuable resources from security incidents (Tryfonas et al., 2001; Canavan, 2003).

It is not enough for organizations to have an ISP. Staff must also comply with it. The factors that affect ISP compliance have been studied extensively as a recent survey demonstrates (Ali et al., 2021). Although some of these studies focus on types of organisations, none on EIS, most are generic based on theories of human behaviour, like the Theory of Planned Behaviour (TPB), Protection Motivation Theory (PMT), Deterrence Theory (DT), etc. They typically take the form of questionnaire-based surveys. Most of them focus on participants' intention to comply with an organisation's ISP, a strong predictor of actual compliance. Comprehensive examples of such studies are (Bulgurcu, et al. 2010; Siponen and Vance 2010). Several studies have shown that attitude towards compliance, a key component of TPB, has a strong influence on people's intension to comply with the ISP (Ifinedo, 2012; Yun and Kim, 2013; Belager 2017). At the same time, several studies emphasise the importance of motivation in ISP compliance, most in the context of PMT and DT (Jai-Yeol, 2011; Ifinedo, 2012; Yoon and Kim, 2013; Sommestad et al., 2014). PMT puts emphasis on perceived risk with fear the main intrinsic/internal motivator, and fear appeals the extrinsic/external motivator. DT theory puts emphasis in the use of sanctions and punishment to deter non-compliance and extrinsically/externally motivate compliance. Both approaches have their limitations. First, studies have shown that intrinsic motivation has a stronger influence on ISP compliance intention rather than extrinsic motivation, but few studies have examined motivation more broadly covering both (Jai-Yeol, 2011; Padayachee, 2012). Second, research in organisations has shown that although sanctions and punishments are effective in motivating passive behaviours, rewards are more effective for active behaviours (Sharot, 2017).

In conclusion, staff attitudes and motivations for ISP compliance in EIS organisations have not been studied to date despite the importance of ISP compliance in securing the personal data they collect and manage. Both intrinsic and extrinsic motivations need to be studied. Of particular interest is the study of positive intrinsic motivations and rewards that have received little attention in the literature to date.

3. RESEARCH METHODOLOGY

To investigate staff attitudes and perceived motivations for ISP compliance in EIS organisations, we focus on the Ghanaian national identification authority (NIA) as a case study, and pose the following research questions:

- What are the attitudes of NIA staff towards ISP compliance?
- What are their perceptions of the intrinsic and extrinsic rewards for ISP compliance?
- Does experience affect ISP compliance attitudes and reward perceptions of NIA staff?

Despite the focus on the NIA, developing countries like Malaysia, Malawi, Nigeria, among others that have similar systems could potentially relate with the findings of this study.

3.1 The Ghanaian National Identification Authority (NIA)

The NIA was established in 2003 with a mandate to register and issue national identity cards to Ghanaian citizens and residents and manage the National Identification System (NIS). The NIA has been issuing citizens and residents with a smart card as a proof of identity that can be used to access basic services such as national health insurance, mobile phone accounts and banking services (Government of Ghana, 2006). The NIS collects and stores the personal data of card holders, including their biometric data.

The NIA management recognised the importance of securing the NIS from the outset. It developed a formally approved information security policy (ISP) and introduced formal ISP awareness training for all staff to boost ISP compliance. More recently, NIA management decided to update the ISP to better match international standards and a revised policy was drafted. However, the revised policy was never formally approved, while formal ISP awareness staff training was suspended until the formal approval.

In the meantime, the NIA has been growing with many staff being hired in recent years. Moreover, the NIA is currently conducting a nationwide identity registration exercise to ensure that all citizens and residents are issued with the national identity card, which has meant that additional staff have been contracted to register the population. Although new staff are made aware of ISP compliance expectations by their line managers, they have not had the clarity of a formal ISP and have not benefited from any awareness training.

The current situation with respect to new staff and the ISP raises some concerns about compliance in light of the personal data that NIS manages and makes the NIA an interesting case to study.

3.2 Study Structure and Procedures

To answer our research questions, similarly to past research, we have designed a questionnaire for NIA non-management staff to elicit their attitudes and their perceptions of motivation towards ISP compliance. Previous work shows that people's attitudes play an important role in determining their intention to comply and actual compliance to ISPs (Bulgurcu et al, 2010). Past research has also shown the significance of intrinsic in addition to extrinsic motivations in ISP compliance (Jai-Yeol, 2011), with focus mostly on negative motivation in terms of sanctions and punishments, and fear (S. Boss et al., 2015). However, positive motivation, intrinsic benefits and extrinsic rewards, has been shown to be more effective in motivating action which we consider essential for identity system organisation staff that must actively protect the personal data they manage (Posey, Roberts, and Lowry, 2015). So, we examine attitudes towards ISP compliance, and perceptions of intrinsic benefits and extrinsic rewards for ISP compliance.

Our questionnaire comprised three scales, one with 4 questions for attitude towards compliance, one with 4 questions for perceptions of intrinsic rewards for compliance, and one with 4 questions for perceptions of extrinsic awards for compliance. The questions were adapted from (Bulgurcu et al, 2010), preserving the actual questions, but using a uniform 7-point Likert scale from Strongly agree to Strongly disagree to conform to Stevens's measurement framework where Likert scale type items are summed or averaged and presented

horizontally (Uebersax, 2006). We also solicited for participants' demographic data (Gender, Age range, Department or Unit, Years of work for the NIA, and Type of employment) to check the representativeness of the sample of employees that participated in the study according to the NIA Human Resources data.

Before distributing the questionnaire, we conducted a pilot study with 10 research students asking for their feedback on our study design. This exposed some minor issues with typographical errors that were corrected.

Due to the unstable nature of the Internet in Ghana, we decided to use paper-based questionnaires to ensure participant access. We printed and distributed 150 questionnaires to NIA staff who were not in managerial positions. To ensure fair participation of all NIA units and departments, we used a distribution formula based on the actual staff strength of each unit or department.

Finally, to conduct the research work, we sought prior ethics approval from our departmental Ethics Committee and obtained approval from the NIA to engage the staff. All participants were over the age of 18 and consented to participate in the study.

4. DATA ANALYSIS AND RESULTS

We obtained 115 questionnaires, 3 of which were excluded from the analysis because they were incomplete. We used the Statistical Package for Social Studies (SPSS) software to carry out our analysis by first, entering the data of the paper questionnaires to Qualtrics. Each participant was assigned a unique identifier. We then grouped each participant's data into Demographic and Non-Demographic Data. The former describes the profile of the participant, while the latter encompass the questions on attitude, perception of intrinsic benefits and perceptions of extrinsic rewards for ISP compliance.

4.1 Participants' Demographics

Table 1 provides an overview of the participants' demographic data (see column Participant Data) compared with NIA Human Resources data (see column Organization Reality). Despite some differences, we consider participants largely representative of the organization's employees.

Table 1. Overview of study demographic data

		Participant Data	Organization Reality
Gender	Male	55.3% (62)	74.0% (172)
	Female	44.6% (50)	26.0% (61)
Age Range	20-30	51.8% (58)	44.9% (96)
	31-40	38.4% (43)	45.8% (98)
	41-50	8.0% (9)	7.0% (15)
	51-60	1.8% (2)	2.3% (5)
Department or Unit	Human Resources	8.0% (9)	2.0% (9)
	Administration	6.3% (7)	52.0% (112)
	Technology and Biometrics	41. 1% (46)	22.0% (48)
	Operations	33.9% (38)	11.0% (35)
	Finance	4.5% (5)	6.0% (12)
	Internal Control	0.9% (1)	1.0% (3)
	Other	3.6% (4)	3.0% (6)
	Procurement	1.8% (2)	2.0 (5)
Years of NIA Work	Less than 1 year	55.4% (62)	32.0% (68)
	1-2 years	12.5% (14)	4.2% (9)
	3-6 years	1.8% (2)	1.4% (3)
	6-9 years	4.5% (3)	1.9% (4)
	More than 9 years	27.7% (31)	60.7% (130)
Employment Type	Permanent	30.4% (34)	64.0% (137)
	Contract	65.2% (73)	33.0% (73)
	Seconded	4.5% (5)	3.3% (7)

4.2 Information Security Policy Compliance Questions

The ISP compliance questions consisted of three scales, attitude towards ISP compliance (4 questions), ISP compliance perceived intrinsic benefits (4 questions), and ISP compliance perceived extrinsic rewards

(4 questions). We evaluated the reliability of these scales using Cronbach's Alpha. Table 2 shows the results that indicate acceptable reliability with Cronbach's Alpha above 0.6. We therefore included all three in our analysis.

Figure 1 shows the distribution of the participants' responses for their attitude towards ISP compliance with 79%, 79%, 85% and 87% of them agreeing that the ISP is necessary, beneficial, important, and useful, respectively, while 17%, 16% 10% and 13% disagreed, and 4%, 5%, 5% and 0% neither agree nor disagree.

Table 2. Summary of reliability analysis

	Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
Attitude towards ISP Compliance	0.654	0.654	4
Intrinsic Benefits of ISP Compliance	0.875	0.878	4
Extrinsic Rewards for ISP Compliance	0.893	0.893	4

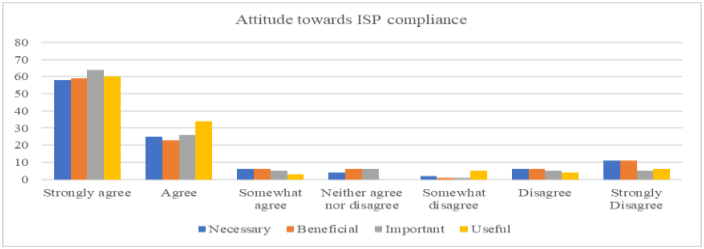

Figure 1. Distribution of participants' responses for attitude towards ISP compliance

Figure 2 shows the distribution for participants' responses for their perceived intrinsic benefits of ISP compliance with most staff agreeing that they feel content (68%), satisfied (73%), accomplished (70%), and fulfilled (69%), when complying with the ISP, while 19%, 13%, 20% and 16% respectively disagreed, and 13%,14%, 11%, and 15% neither agreed nor disagreed.

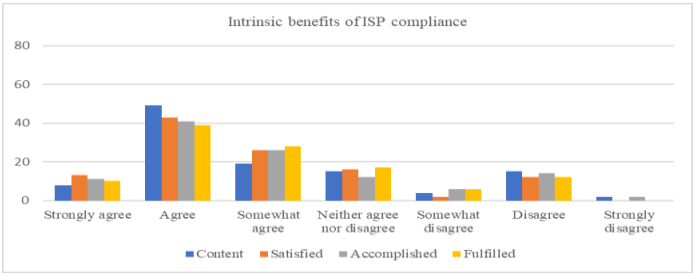

Figure 2. Distribution of participants' response for intrinsic benefits of ISP compliance

Figure 3 shows the distribution for participants' responses for their perceived extrinsic rewards for ISP compliance with the majority disagreeing that their ISP compliance will be rewarded in monetary/non-monetary (57%) or tangible/non-tangible awards (51%), with only 29% and 32% agreeing, and 17% and 14% neither agree nor disagree respectively. In addition to this, more participants disagree that their compliance will be rewarded with a pay rise/promotion (46%) than agree (35%), and the rest (19%) neither agree nor disagree. In contrast, more participants agree that their compliance will be rewarded with a personal mention/written assessment report (43%) than disagree (38%), and the rest (19%) neither agree nor disagree.

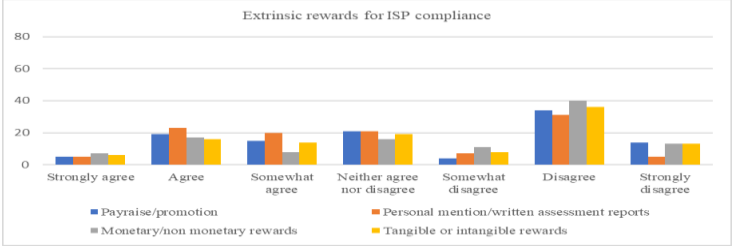

Figure 3. Distribution of participants' response for extrinsic rewards for ISP compliance

Comparing the first three figures we can say that, overall, although participants' attitudes and perceived intrinsic benefits of ISP compliance are positive, the former is much more positive than the latter. In contrast, their perceptions of extrinsic rewards for ISP compliance are negative. This is also supported by Table 3 which shows the Means and standard deviations for the corresponding questions with numbers below 4 indicating participant agreement levels with lower values indicating stronger agreement, while those above 4 indicate disagreement, with higher values indicating stronger disagreement.

Table 3. Means and standard deviations for the survey questions

		Mean	Std. dev.
Attitude towards ISP compliance	Necessary	2.37	2.022
	Beneficial	2.37	2.022
	Important	2.01	1.663
	Useful	1.99	1.636
Intrinsic benefit of ISP compliance	Content	3.10	1.582
	Satisfied	2.88	1.425
	Accomplished	3.10	1.582
	Fulfilled	3.05	1.432
Extrinsic rewards for ISP compliance	Pay rise/promotion	4.41	1.858
	Personal mention/written assessment report	4.03	1.732
	Monetary/non-monetary rewards	4.60	1.867
	Tangible/intangible rewards	4.49	1.836

Table 4. Means and standard deviations for the survey questions for experienced and inexperienced participants

		Experienced		Inexperienced	
		Mean	Std. dev.	Mean	Std. dev.
Attitude towards ISP compliance	Necessary	2.33	1.690	2.38	2.172
	Beneficial	2.36	1.743	2.37	2.153
	Important	2.25	1.746	1.89	1.621
	Useful	2.31	1.721	1.84	1.584
Intrinsic benefit of ISP compliance	Content	3.81	1.833	2.76	1.335
	Satisfied	3.22	1.726	2.72	1.239
	Accomplished	3.33	1.773	2.99	1.483
	Fulfilled	3.36	1.693	2.91	1.277
Extrinsic rewards for ISP compliance	Pay rise/promotion	5.44	1.594	3.92	1.780
	Personal mention/written assessment report	4.81	1.582	3.66	1.686
	Monetary/non-monetary rewards	5.42	1.538	4.21	1.838
	Tangible/intangible rewards	5.22	1.623	4.14	1.838

Table 5. T-test for inexperienced vs. experienced staff for extrinsic rewards for ISP compliance

	T	Df	Significance		Mean Difference	Std. Error Difference	95% Interval Difference	Confidence of the
			One-Sided p	Two-Sided p			Lower	Upper
Pay rise/promotion	-4.548	76.16	<.001	<.001	-1.523	0.335	-2.191	-0.856
Personal mention/written assessment report	-3.509	72.908	<.001	<.001	-1.148	0.327	-1.799	-0.496
Monetary/non-monetary rewards	-3.591	83.25	<.001	<.001	-1.206	0.336	-1.874	-0.538
Tangible/intangible rewards	-3.141	77.149	0.001	0.002	-1.077	0.343	-1.76	-0.395

We classified staff into two groups, experienced and inexperienced, based on the number of years they have been working for the NIA. Those working for 3 years, or more were classified as experienced and those with less than 3 years classified as inexperienced. Table 4 shows the means and standard deviations for the two groups across all the survey questions. There is a clear difference in the mean responses of experienced and inexperienced staff for their perceived extrinsic rewards for ISP compliance with inexperienced staff neither agreeing nor disagreeing while experienced staff disagreed. T-tests indicate that the difference is statistically significant with $p<0.05$, see Table 5. For perceived intrinsic benefits of ISP compliance, both experienced and inexperienced staff agree, with inexperienced staff in more agreement than experienced staff (i.e., lower means). However, t-tests show that the only difference is for feeling content which is statistically significant with $p<0.05$ ($t=-3.05$, $df=53.233$, one-sided $p=0.002$, two-sided $p=0.004$, mean difference=-1.042, std.

error=0.342. and 95% Confidence Interval of the Difference (-1.728, -0.357)). Finally, for both attitude towards ISP compliance both experienced and inexperienced staff agree with small means' differences that t-tests show aren't statistically significant.

5. DISCUSSION

The results are encouraging overall for the NIA. The attitude of NIA staff towards ISP compliance and their perceptions of the intrinsic benefits for it are positive, and literature shows that these are important factors for compliance (Bulgurcu, et al. 2010; Jai-Yeol, 2011). It is also reassuring that this is the case for both experienced staff who benefited from a formally approved ISP policy and ISP awareness training in the past, and inexperienced staff that lacked these benefits. In contrast, the NIA staff perceptions of the extrinsic benefits for ISP compliance are negative. This reflects the fact that the NIA is subjected to rigid government control procedures on financial budgetary allocations which include no officially accepted rewards for ISP compliance. Although in principle, it is possible for managers to offer financial incentives, these require the approval of both the board of Directors of the NIA, and the Parliament of Ghana or the government in power. Without such approval management is liable for misapplication or misappropriation of public funds. Although informal rewards like positive mentions either in personal or written assessment reports are possible, these are not as common, reflecting the fact that NIA management places more emphasis on deterrence. The statistically significant difference between experienced and inexperienced seems to result from lack of clarity on extrinsic awards for inexperienced staff, that could have been avoided if ISP awareness training was in place. Overall, extrinsic rewards is an area for improvement for the NIA, both in terms of providing more clarity to new staff and adopting a more balanced motivational approach between deterrence and rewards, going potentially as far as to introduce compliance as part of promotion decisions and financial reward packages.

Looking beyond the NIA for EIS organisations, our findings highlight the importance of clarity regarding the extrinsic motivation of staff for ISP compliance through formally approved ISP policy and ISP awareness training, especially for new staff. Although such training can also be beneficial in terms of attitude and intrinsic motivation, one should not forget that research shows that social factors can also promote a positive security culture in organisations (Warkentin and Johnston, 2010). More research is needed in establishing what the right balance between sanctions and rewards should be.

The main limitation of our work is that it focused on the NIA and the situation it currently faces with respect to the lack of formally approved ISP and ISP awareness training. Although we believe that the situation is not uncommon for EIS organisations as they grow, more research is needed to further validate our findings. The research will have been stronger if the questionnaire findings were combined with actual compliance monitoring to establish how attitudes and perceptions relate to tangible information security protection.

6. CONCLUSION AND FUTURE WORK

This paper presents the first study on attitude towards compliance and perceived motivations for ISP compliance in EIS through a case study of the NIA. The study explored perceived intrinsic benefits and perceived extrinsic rewards for ISP compliance. The study shows that despite the lack of formally approved ISP and ISP awareness training, there is a positive information security culture in the NIA with staff recognising the necessity, benefits, importance, and usefulness of the ISP and feeling content, satisfied, accomplished, and fulfilled when complying with it. However, things are less clear with extrinsic rewards. Although experienced staff perceptions are clear that, extrinsic rewards do not motivate compliance, inexperienced staff are unclear. This is where the lack of ISP awareness training is negatively impacting the NIA information security culture.

The study findings further reinforce the need for clarity in EIS organisations with a formally approved ISP and ISP awareness training. They also highlight an opportunity in complementing sanctions with rewards for extrinsic motivation of their staff and further cultivation of a positive information culture.

In terms of future work, similar research could be conducted in other EIS organisations to ascertain the generalizability of this research finding. Moreover, as this research focused on only non-management staff of the NIA, future research work could focus on the views of NIA management and external stakeholders.

REFERENCES

Ali, R.F. et al., (2021). *Information Security Behaviour and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance*, Applied Sciences, vol. 11, no. 3383, https://doi.org/10.3390/app11083383.

Alzahrani, A. et al., (2018). *Information security policy compliance: Investigating the role of intrinsic motivation towards policy compliance in the organisation*. In 4th International Conference on Information Management, pp. 125-132.

Belager, F. et al., (2017), *Determinants of early conformance with information security policies*. Information Management, vol. 54, pp. 887-901.

Boss, S. et al., (2015). *What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors*, MIS Quarterly, vol. 39, pp. 837–864.

Bulgurcu, B. et al. (2010). *Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*, MIS Quarterly, pp. 523-548.

Canavan, S. (2003). *An information security policy development guide for large companies*, SANS Institute.

Flowerday, S. V. and Tuyikeze, T. (2016). *Information security policy development and implementation: The what, how and who*. Computers and Security, vol. no.61, pp. 169-183.

Government of Ghana, (2006). *National Identification Authority Act*, Act 707, Parliament of the Republic of Ghana, Accra, Ghana.

Handforth, C. and Matthew, W. (2019). *Digital Identity Country Report:* Malawi, available online at https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf, last accessed 25/08/2019.

Ifinedo, P. (2012). *Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory*, Computers and Security, vol. 31, pp. 83-95.

Jai-Yeol, S. (2011). *Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies*, Information Management, vol. 48, pp. 296–302.

Johnson, E. C. (2006). *Security Awareness: Switch to a better programme*, Network security, vol.2, pp. 15-18.

Lyon, D. and Bennett, C. J. (2013).1 *Playing the ID Card: Understanding the significance of identity card systems*, in Playing the identity card: Surveillance, security and identification in global perspective, pp. 3-20.

Raggad, B. G. (2010). *Information security management: concepts and practice*, CRC Press.

Sharot, T. (2017). *What Motivates Employees More: Rewards or Punishments?* Harvard Business Review, available online at https://hbr.org/2017/09/what-motivates-employees-more-rewards-or-punishments, Last accessed 05/01/22023.

Siponen, M. and Vance, A. (2010). *Neutralization: New insights into the problem of employee information systems security policy violations*, MIS Quarterly, pp. 487-502.

Sommestad, T. et al., (2014). *Variables influencing information security policy compliance*. Information Management and Computer Security, vol. 22, *pp. 42–75.*

Padayachee, K. (2012). *Taxonomy of compliant information security behavior*, Computer Security, *vol.* 31, *pp. 673–680.*

Posey, C. Roberts, T.L. and Lowry, P.B. (2015). *The impact of organizational commitment on insiders' motivation to protect organizational information assets*. Journal of Management Information Systems, 32(4), 179-214.

Tryfonas, T. et al., (2001). *Embedding security practices in contemporary information systems development approaches*, Information Management and Computer Security, vol. 9, pp. 183-197, 2001.

Uebersax, J. S. (2006). *Likert scales: dispelling the confusion*, Statistical methods for rater agreement, vol. 31.

Warkentin, M. and Johnston, A.C. (2010). *Fear appeals and information security behaviors: An empirical study*. MIS Quarterly, vol. *34*, pp. 549–566.

Wladawsky-Berger, I. (2016). *Towards a Trusted Framework for Identity and Data Sharing*, https://blog.irvingwb.com/blog/2016/11/trusted-identity-and-data-ecosystems.html Accessed October 20, 2019.

Yoon, C. and Kim, H. (2013), *Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms*, Information Technology and People, vol. *26*, pp. 401–419.