Information Security Policy Awareness Beliefs versus Reality in Electronic Identity Systems

A Case Study of the Ghanaian National Identity System

Salim Awudu, Dr Sotirios Terzis
Department of Computer and Information Sciences, University of Strathclyde,
Glasgow, United Kingdom
{salim.awudu, sotirios.terzis}@strath.ac.uk

***Abstract*— Electronic Identity Systems (EIS) have become a tool for economic, social, and political development in several countries. However, certain concerns by governments or their citizens have impeded wider adoption. These concerns are about EIS trustworthiness, privacy, and security. An effective Information Security Policy (ISP) can be key in addressing these concerns provided staff are aware and understand it provisions. A lot of work has been done on general ISP awareness in organizations, but little attention has been given to ISP awareness in electronic identity systems. Moreover, people's awareness of these policies in organizations is typically measured with instruments that focus on staff beliefs about their knowledge and understanding of ISP provisions rather than their actual understanding and their ability to translate ISP provision into protective behaviors. Staff belief is generally about how staff ISP awareness is typically measured while real awareness is about the prescribed behaviors of the staff. Using the Ghanaian National Identification Authority (NIA) as a case study, this paper examines the relationship between staff beliefs about ISP awareness and the reality of knowing and understanding the prescribed behaviors. A questionnaire study was conducted with scales from literature, which shows that NIA staff beliefs match the reality, despite the lack of a formal ISP and staff training. The study also indicates that a formal ISP and training can enhance staff understanding and confidence in their knowledge. It also shows that for EIS it is important that their ISP considers the organizational context.**

Keywords: electronic identity systems; trustworthiness; information security policy (ISP) awareness; ISP common violations

I. Introduction

Several countries and organizations depend on Electronic Identity Systems (EIS) to identify, authenticate, and verify their citizens and customers. These systems process identity data about individuals to create value for organizations, businesses and individuals through verified identities [17]. Although these systems are used to achieve economic, social, and political purposes, there are increasing concerns about the security, privacy, and trustworthiness of these systems and the collected personal data [5]. According to Flowerday and Tuyikeze [3] “one important mechanism for protecting organizations’ assets is the formulation and implementation of an effective ISP”. Staff awareness of ISP provisions and their actual knowledge and understanding of them are key for its effectiveness, especially so for EIS that manage personal data. Effective protection of the sensitive data managed by EIS relies on knowing and understanding what protective behaviors are prescribe by the EIS ISP. However, research to date tends to measure ISP awareness using instruments that measure staff beliefs about their knowledge and understanding. This introduces a risk for EIS in that staff beliefs may not match their actual understanding of the protective behaviors prescribed. Prescribed behaviors are actions or inactions that are specified in the ISPs of organizations. So, for EIS it is essential to ensure that staff beliefs about ISP awareness match their knowledge and understanding in the ISP.

This paper investigates the relationship between staff belief of ISP awareness and the reality of their knowledge and understanding using the Ghanaian NIA as a case study. A questionnaire-based study was conducted using scales from literature for ISP awareness and understanding of common ISP violations for non-managerial staff of the NIA. The study finds that despite the particular NIA setting, where there is no formal ISP and no training provided, staff do not only believe that they know and understand the provisions of the NIA ISP but can identify common ISP violations as violations of NIA ISP. The study also shows that there is some room for improvement in staff understanding and confidence through ISP formalization and training. The study also indicates that, for the ISP of EIS, it is important to also consider the organizational context. Additional studies following alternative research approaches can be used to confirm these findings, while further studies in other EIS organizations can help generalize them.

We begin the paper with related work on EIS and ISPs, in II before we describe our methodology in III, and present our analysis and findings in IV, followed by a discussion in V, and finally conclude the paper with the identification, and directions for future work in VI.

II. Related Work

EIS are systems that are built to collect, process, store and use personal data or information about individuals in a defined area or territory for the purpose of planning or providing services to the people both within the defined territory and beyond [9]. EIS can also be seen as “system[s] that involve the collection of information or attributes associated with a specific entity” [15]. Several countries, including

Ghana, have fully operationalized an electronic identity system.

Despite the potentially immense benefits of EIS, several people have reservations about the potential negative effects they can cause. For instance, Lyon and Bennett note that "once cards are mandatory, then they may be used to single out or even to harass visible minorities and those with alternative lifestyles" [7]. Further concerns are about Privacy, Trustworthiness, Confidentiality, Integrity, and Availability [10], especially as EIS present an appealing target for attackers because of data that they collect, store, and manage. So, information security assurance is essential for EIS.

According to Von Solms [14], information security (IS) is largely multi-dimensional, and organizations must consider all aspects to ensure the security or protection of their information assets and environment. This "includes the physical security of buildings, fire protection, software and hardware, personnel policies and financial audit and control" [16]. Furnell et al. [4] pointed out that employee attitudes and lack of security awareness are the most notable contributors to security incidents. To prevent such incidents, Johnson [6] identified the need for organizations to have an information policy that reflects local information security philosophy and commitments. According to Tryfonas et al. [12] and Canavan [2] 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. Organizations need to have an ISP and ensure staff are aware and comply with it, because Sipponen and Vance [11] have shown that violations of security policies occur through user's negligence or ignorance of the ISP provisions. Staff understanding and appreciation of ISP provisions is key.

Although a lot of work has been on ISP awareness, e.g. [1, 11], in general, there has been little attention to ISP awareness in EIS. Moreover, instruments to measure ISP awareness, like the one proposed in [1], tend to focus on the beliefs of staff about their ISP knowledge and understanding without any attempts to investigate whether these beliefs reflect actual knowledge and understanding of the protective behaviors prescribed by the ISP.

In this context, for any organization it is important to investigate whether staff beliefs about their awareness of ISP provisions match their actual knowledge and understanding. This is especially the case for EIS where information security is a necessity.

III. RESEARCH METHODOLOGY

To investigate the relationship between beliefs about awareness and actual knowledge and understanding of ISP provisions in the context of EIS, we pose the following research questions: 1) Do EIS staff believe they are aware of the rules, regulations and responsibilities prescribed by the ISP of their organization? and 2) Do EIS staff appreciate key provisions of their organization's ISP?

To explore these questions, we focused our investigation on the Ghanaian National Identification Authority. Despite this, we believe that other countries with similar digitized EIS like Malaysian, Malawian, Nigeria, among others could potentially associate with the findings of this research work.

A. The NIA

The NIA was established in 2003 with the mandate to issue national ID cards to both citizens and residents as well as to manage the National Identification System (NIS). The Ghanaian Identification System is a digitized one where personal data of citizens and residents are collected and stored. The applicants are issued with a smart card to enable them to prove their identity when accessing basic services like mobile phone Subscriber Identity Module (SIM) card registration and banking services [8]. Currently, the NIA is issuing biometric identity cards throughout the country. While this is ongoing, telecommunication companies and banking institutions are required by law to reregister all customers by demanding the national ID card as proof of identity.

Protecting collected citizens data is seen as an essential part of the NIA mission. So, at the outset the organization established an ISP specifying relevant requirements for its staff and introduced training for them. Over time, some updates to the ISP were deemed necessary and a revision was carried out. However, the revised ISP has not been formally approved and there is currently no information security training provided to staff. This situation is concerning for the security of citizens' and residents' data making the NIA an interesting case study to investigate its staff perceptions and the reality of its ISP awareness.

B. Study structure and Procedures

We designed a questionnaire to solicit the views of NIA staff about their awareness of the ISP provisions and to compare them against their understanding of what constitute typical policy violations. This allowed us to assess whether staff beliefs about their knowledge translate into actual knowledge.

More specifically, the questionnaire comprised two scales, one for ISP awareness consisting of 3 questions and adopted from Bulgurcu et al. [1], and one about common ISP violations with 9 questions adopted from Siponen and Vance [11]. Both scales use a Likert scale from Strongly agree to Strongly disagree. However, although we preserved the actual questions, we adapted them to a uniform 7-point Likert scale, which conforms to Stevens's measurement framework where Likert scale type items are summed or averaged and presented horizontally [13].

In additions to the two scales, we also solicited demographic data from participants (Gender, Age range, Department or Unit, Years of work, Educational background, and Type of employment) to check whether the participants form a representative sample of the organization's employee population as captured in NIA Human Resource Data.

C. Study Procedures

Prior to the study, ethics approval was obtained from our department's Ethics Committee. We also obtained approval from the NIA to engage the staff.

We conducted a pilot study with 10 research students at our department and asked for their feedback, which was used to improve the study design before the main data collection exercise. This uncovered some minor issues with typographical errors that were corrected.

During the main data collection exercise, we printed and distributed 150 questionnaires randomly to staff of the NIA who are not in managerial positions. After the distribution, 115 questionnaires were returned. Three questionnaires were excluded because they were incomplete.

To ensure fair participation from each unit or department, a distribution formula was used. The distribution formula was primarily developed based on the actual staff strength of each unit or department.

We used paper-based questionnaires to ensure easy access to participants to avoid problems with unstable internet connectivity in some of the districts that the data was collected from. All participants were over the age of 18 and consented to participate in the study.

IV. Data Analysis and results

To facilitate analysis with the Statistical Package for Social Studies (SPSS) software, the data of the paper questionnaires were entered to Qualtrics, and each participant was assigned a unique identifier. For the analysis, each participant's data was divided into Demographic and Non-Demographic Data. The former describes the profile of the participant, while the latter, the information security questions that are the focus of the research.

A. Participants' Demographics

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

TABLE I: OVERVIEW OF STUDY DEMOGRAPHIC DATA.

		Participant Data	**Organization Reality**
Gender	Male	54% (60)	74.0% (172)
	Female	46% (56)	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% (5)	2.0% (9)
	Administration	6.3% (7)	52.0% (112)
	Technology and Biometrics	41. 1% (47)	22.0% (48)
	Operations	31.3% (24)	11.0% (35)
	Finance	3.6% (4)	6.0% (12)
	Internal Control	2.7% (3)	1.0% (3)
	Other	2.7% (3)	3.0% (6)
	Procurement	4.5% (5)	2.0 (5)
Years of Work	Less than 1year	55.4% (62)	32.0% (68)
	1-2years	12.5% (14)	4.2% (9)
	3-9years	4.5% (5)	3.3% (7)
	More than 9years	27.7% (41)	60.7% (130)
Employment Type	Permanent	30.4% (34)	64.0% (137)
	Contract	65.2% (70)	33.0% (73)
	Seconded	4.5% (5)	3.3% (7)

B. Information Security Questions

The information security questions consisted of two scales, ISP Awareness (3 questions) and Most Common ISP Violations (9 questions). We evaluated the reliability of these two scales using Cronbach's Alpha as the measure of reliability. Table II shows the results that both measures have acceptable reliability with Cronbach's Alpha above 0.8, so both are included in the analysis. We look more closely at the results for each scale in the following sections.

TABLE II: SUMMARY OF THE CRONBACH ALPHA

	Cronbach's Alpha	**Cronbach's Alpha Based on Standardized Items**	**No. of Items**
ISP Awareness	0.915	0.915	3
Most Common ISP Violations	0.876	0.882	9

C. ISP Awareness

Figure 1 shows how participant responses are distributed for the 3 ISP awareness questions. Most of the staff agree that they know (86%) and understand (80%) the provisions of the NIA ISP and know the responsibilities it prescribes (84%). However, some disagree (9%, 12%, 10% respectively) while others are unsure (5%, 7%, 7% respectively).

Looking more closely at those that disagree, we wanted to see whether there is any commonality in their characteristics. So, we looked at their gender, experience (considering those working for the NIA for 3 or more years as experienced and those less than 3 years as inexperienced), and department or unit. As we can see in Table III, there are more female than male participants that disagree, with a mix of experienced and inexperienced employees. These participants were also from a range of different departments and units (we do not show these numbers due to space limitations). As a result, there is no clear pattern in the characteristics of these participants that may explain their response.

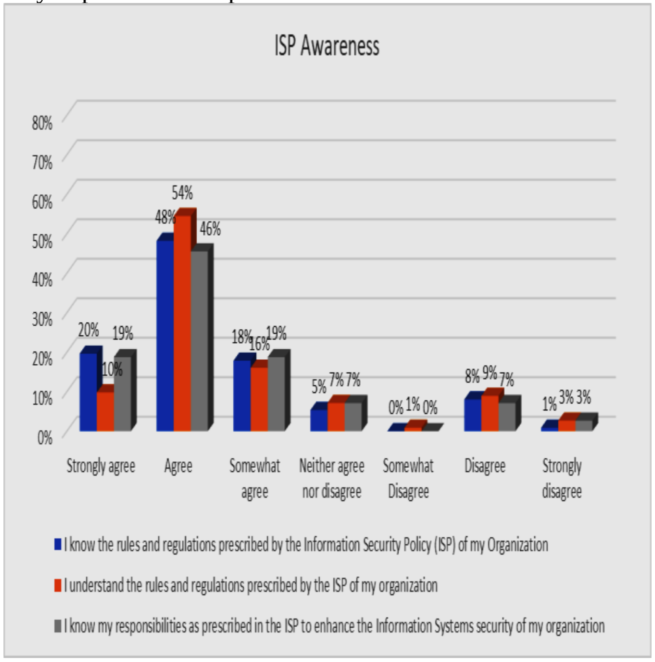

Figure 1: ISP Awareness.

TABLE III: ISP AWARENESS CHARACTERISTICS OF DISAGREEING PARTICIPANT.

ISP Knowledge		
Gender	**Experience**	**Count**
Male	Experienced	1
Female	Experienced	4
	Inexperienced	4
ISP Understanding		
Gender	**Experience**	**Count**
Male	Inexperienced	2
Female	Experience	4
	Inexperienced	4
Knowledge of Responsibilities		
Gender	**Experience**	**Count**
Male	Experienced	1
	Inexperienced	1
Female	Experienced	4
	Inexperienced	2

D. *Most Common ISP Violations*

Figures 2a, 2b and 2c are distributed for the 9 most common ISP violations questions. We have grouped these questions thematically with Figure 2a showing information transfer-related violations, Figure 2b password-related ones, and Figure 2c workstation-related ones.

From the figures, one can see that in all cases most participants agree that these are NIA ISP violations with information transfer-related violations 95%, 92% and 84%, password-related violations 84%, 89% and 91%, and workstation-related violations 88%, 90% and 91, respectively. Again, some participants disagree 1%, 4%, 8% for information transfer-related violations, 8%, 2%, 5% for password-related violations, and 5%, 6%, 4% for workstation related violations respectively. Other participants are unsure 4%, 4%, 8% for information transfer related violations, 8%, 9%, 5% for password related violations, and 7%, 4%, 6% for workstation-related violations, respectively.

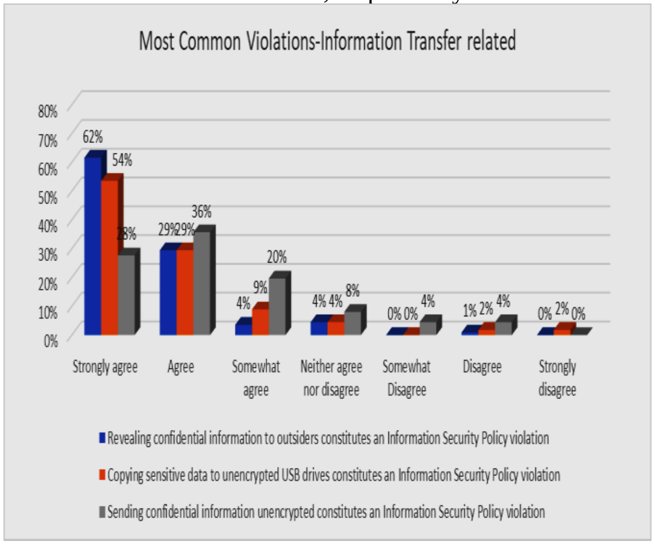

Figure 2a: Most Common Information Transfer-related ISP Violations.

Looking more closely at Figure 2a, Figure 2b and Figure 2c, we note that despite the very high overall agreement with all the violations, there are clear differences in the distributions which indicate differences in the degree of agreement between them. To tease out these differences we treated the Likert scales as ratios from 1 for Strongly agree to 7 for Strongly disagree and we calculated the mean and standard deviation for each of them, see Table IV. The table shows that the means for the common ISP violations range from 1.54 to 2.39 with standard deviations between 0.879 to 1.537. Three of the violations "Creating easy to guess passwords", "Using laptops carelessly outside" and "Failing to lock or log out" have means above 2, 2.39, 2.21, 2.03 respectively, with the former two also having the highest standard deviations, 1.331 and 1.537 respectively. As a result, indicating the agreement to these constitute NIA ISP violation is not as strong as the rest.

Finally, looking at how the means and standard deviations of the common ISP violation questions compare to those of the awareness questions, Table IV shows that the latter have higher means ranging from 2.46 to 2.72 and standard deviations between 1.381 and 1.490. These indicate that agreement with the awareness questions is not as strong to the common ISP violations.

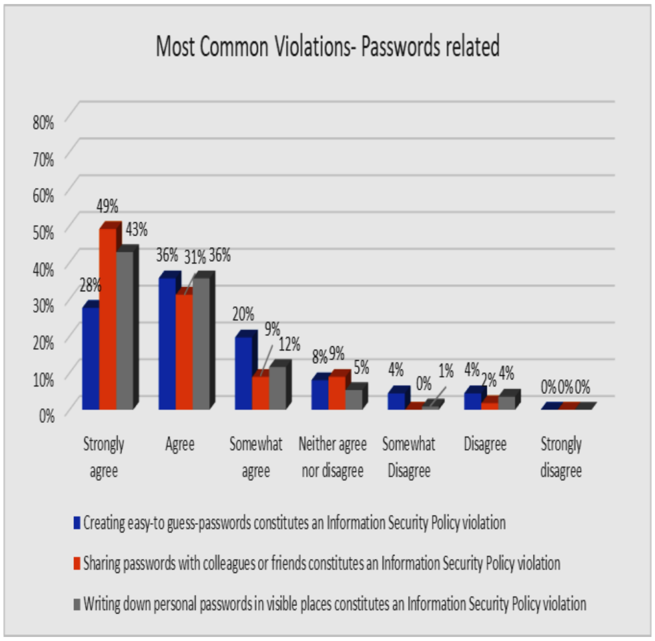

Figure 2b: Most Common Passwords-related ISP violations.

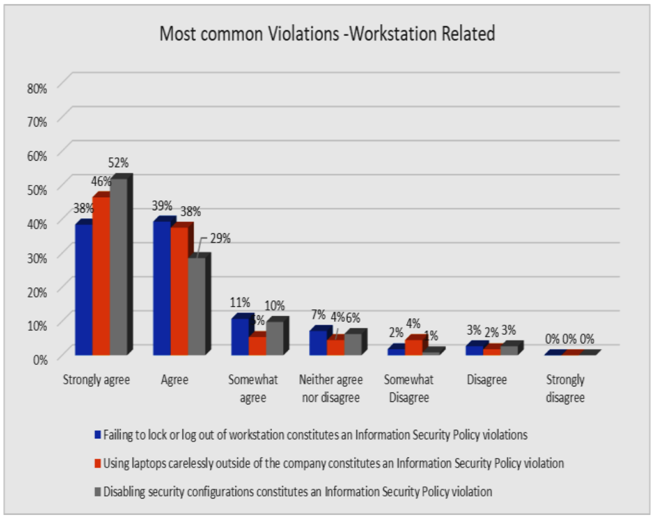

Figure 2c: Most Common Workstation-related ISP Violations.

V. Discussion

Overall, our findings are reassuring for the NIA. Despite the lack of a formal ISP and any staff training on information security, our results show that staff believe they know and understand what is expected from them. More importantly, this is not just their perception. Their understanding of common ISP violations demonstrates that they appreciate their role and responsibilities in protecting NIA information security, an indicator of a good security culture.

That said, there is some room for improvement. First, our results show that for certain violations, NIA staff agreement is not as strong as for others. In some cases, such differences are indicative of typical tensions between security and usability. For example, logging out or locking workstations can slow down work, while coming up with passwords that are not easy to guess can be challenging. In such cases, staff training can help staff identify good strategies for managing these tensions. In other cases, the differences are indicative of lack of clarity in what is and isn't acceptable. For example, NIA staff often use their personal laptops for work and with the absence of a formal ISP they may be unclear of what constitutes careless use. In such cases, a formal ISP with coverage of bring-your-own-device expectations can help staff ensure that, the use of their laptops does not compromise organizational security. Moreover, combining a formal ISP with relevant staff training can also increase the confidence of NIA staff in their knowledge and understanding further strengthening the information security culture of the organization.

TABLE IV: MEANS AND STANDARD DEVIATION OF ALL INFORMATION SECURITY RELATIONS.

	Mean	Std. Deviation
I know the rules and regulations prescribed by the Information Security Policy (ISP) of my organization	2.46	1.381
I understand the rules and regulations prescribed by the ISP of my organization	2.72	1.490
I know my responsibilities as prescribed in the ISP to enhance the Information Systems security of my organization.	2.56	1.475
Failing to lock or log out of workstation constitutes an Information Security Policy violation	2.03	1.174
Writing down personal passwords in visible places constitutes an Information Security Policy violation	1.96	1.193
Sharing passwords with colleagues or friends constitutes an Information Security Policy violation	1.85	1.100
Copying sensitive data to unencrypted USB drives constitutes an Information Security Policy violation	1.80	1.229
Revealing confidential information to outsiders constitutes an Information Security Policy violation	1.54	0.879
Disabling security configurations constitutes an Information Security Policy violation	1.84	1.167
Using laptops carelessly outside of the company constitutes an Information Security Policy violation	2.21	1.537
Sending confidential information unencrypted constitutes an Information Security Policy violation	1.88	1.176
Creating easy-to guess-passwords constitutes an Information Security Policy violation	2.39	1.331

For Electronic Identity Systems, our research reinforces the need for a formal ISP that clearly specifies requirements for staff. It also emphasizes the importance of staff training ensuring that policy provisions are fully appreciated and understood. In addition to this, it highlights the necessity to consider the organizational context in the development and implementation of the ISP.

The main limitation of our research is the focus on staff of the NIA. This limits the generalizability of our findings. Similar studies in other organizations are necessary to generalize them. In addition to this, our research was questionnaire based. This limits the extent to which we can extrapolate from our findings, the information security behaviors of NIA staff. This would require an observation study to establish whether staff behave in ways to prevent ISP violations. Finally, the research focused on NIA staff in non-management positions. This means that the research is unable to incorporate management's view in the study and whether management views agree with those captured in the study. As a result, our findings are limited to such staff and do not include management views. Surveying management views will address this.

VI. Conclusion and Future Work

We conducted a questionnaire-based study using the Ghanaian NIA as a case. The study shows that although there is no formal ISP and no staff training there is a positive information security culture where staff not only believe they are aware of the ISP provisions but can identity common ISP violations of the NIA ISP. Our study reinforces the need for a formal ISP in EIS and training as the means for clarifying requirements and enhancing staff knowledge and understanding. It also highlights the need to consider the organizational context in the development and implementation of the ISP.

In addition to addressing the limitations above, future work could explore in more detail, the implementation of information security policy at the NIA by looking at how engaged staff are in the development and evolution of its provisions and how compliance is enforced.

Again, similar research works could be replicated in other regions or countries to assess the generalizability of this research findings in other jurisdictions

The impact of covid 19 pandemic also affected the research work. As at the time the data was being collected, the government-imposed restrictions on work attendance and this partly led to rotation of staff attendance. This in effect affected the period for the data collection exercise. In the future, such research work might need to consider longer time due to incorporate such natural occurrences.

References

[1] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness”, *Management Information Systems Quarterly*, pp. 523-548, 2010 https://doi.org/10.2307/25750690

[2] S. Canavan, "An information security policy development guide for large companies." SANS Institute,2003.

[3] S. V. Flowerday, and T. Tuyikeze, “Information security policy development and implementation: The what, how and who”, *Computers & Security*, pp. 169-183, 2016.

[4] S. M. Furnell, P. Bryant, and A. D. Phippen “Assessing the security perceptions of personal Internet users”, *Computers & Security*, Vol. *26, no.*5, pp. 410-417, 2007.

[5] C. Handforth, and W. Matthew, “Digital Identity Country Report: Malawi” 2019 Available: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report.pdf [Accessed August, 25, 2019].

[6] E. C. Johnson, “Security Awareness: Switch to a better programme”, *Network security, Vol.*2, pp. 15-18, 2006.

[7] D. Lyon, and C. J. Bennett, “Playing the ID Card: Understanding the significance of identity card systems: Playing the identity card: Surveillance, security and identification in global perspective”, pp. 3-20, 2008.

[8] National Identification Authority Act, Government of Ghana, “National Identification Authority Act, 2006 Act 707”, In: Ghana, G. O. (Ed.) Act 707. Accra: Parliament of the Republic of Ghana, 2006.

[9] National Identification Authority, “NIA Draft Policy 2014” n.d Accra

[10] B. G. Raggad, “Information security management: concepts and practice”, CRC Press,2010.

[11] M. Siponen, and A. Vance, “Neutralization: New insights into the problem of employee information systems security policy violations” *MIS quarterly*, pp. 487-502, 2010.

[12] T. Tryfonas, E. Kiountouzis, and A. Poulymenakou, “Embedding security practices in contemporary information systems development approaches*”, Information Management & Computer Security*, Vol. 9, pp. 183-197, 2001.

[13] J. S. Uebersax, “Likert scales: dispelling the confusion” *Statistical methods for rater agreement*, Vol. *31, 2006*.

[14] R. Von Solms, "Information security management: why standards are important", *Information Management & Computer Security, 1999*.

[15] I. Wladawsky-Berger, (2016), “Towards a Trusted Framework for Identity and Data Sharing”, 2016. [Accessed October 20, 2019].

[16] C. C. Wood, “Writing infosec policies” *Computers & Security*, Vol. 5, pp. 418, 1995.

[17] World Economic Forum, “Identity in a digital world – A new chapter in the social contract” Cologny/Geneva: World Economic Forum, 2018.