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

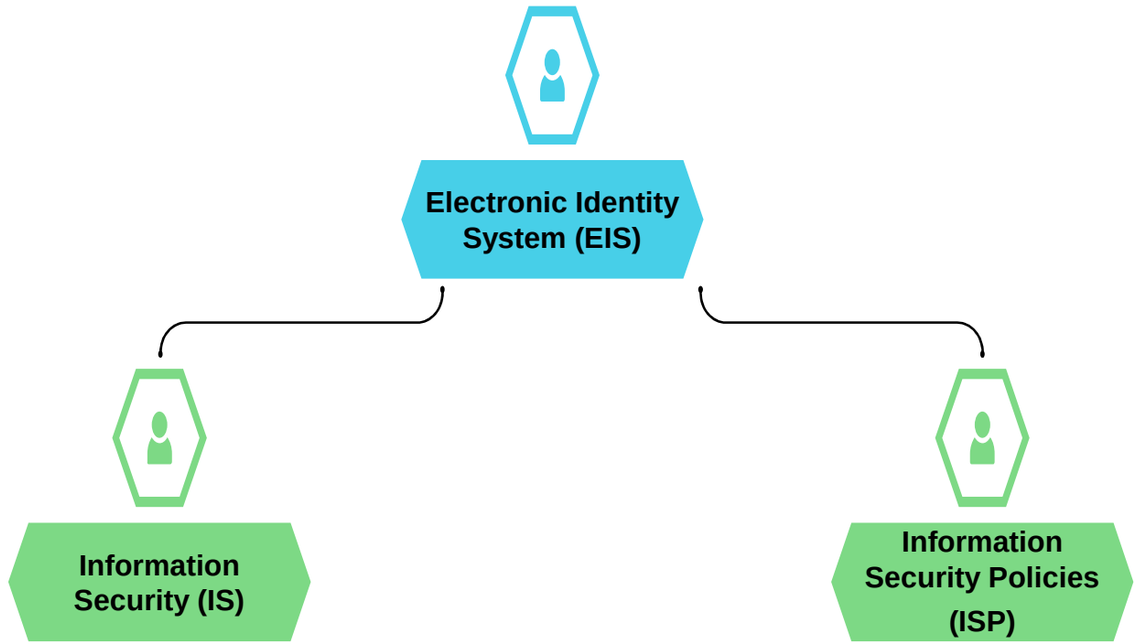
Table of Content

Electronic Identity Systems (1)

- Electronic Identity Systems (EIS) have been used as a tool for economic, social and political development
- Privacy, trustworthiness and security concerns raised by government and citizens
- Information Security Policies (ISPs) are a tool in addressing such concerns through awareness and understanding of the policy provisions

Electronic Identity Systems (2)

- EIS “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” (NIA Draft Policy, 2014)
- Information security (IS) includes “the physical security of buildings, fire protection, software and hardware, personnel policies and financial audit and control” (Wood, 2016)
- 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)



Research Problem & Questions

- ISP awareness is typically measured by staff beliefs, but real awareness is about the behaviours prescribed for staff
- For EIS it is essential to ensure that staff beliefs about ISP awareness match their knowledge and understanding
- RQ1: Do staff believe they are aware of the rules, regulations and responsibilities prescribed by the ISP of their organization?
- RQ2: Do staff appreciate key provisions of their organization’s ISP?

Research Methodology (1)

- Questionnaire based investigation on staff awareness beliefs versus real ISP awareness using the Ghanaian National Identity Authority (NIA) as a case study

- NIA was formed in 2003 with mandate to manage the national identity system and issue biometric cards to both citizens and residents(temporal and permanent)
- The NIA collects and stores personal data of citizens and residents and issues biometric identity cards throughout the country
- Telecommunication companies and banking institutions are required by law to reregister all customers by demanding the national ID card as proof of identity
- The national identity system is typical to the ones in other countries like Malaysia, Malawi, Nigeria, etc

- Protecting collected citizens data is seen as an essential part of the NIA mission
- From the outset the NIA established an ISP specifying relevant requirements for its staff and introduced training for them
- A revised information security policy for the NIA was drafted but was not formalised

Research Methodology (2)

- Study structure
  - 3 questions on awareness of the ISP provisions adopted from (Bulgursu et al. 2010)
  - 9 questions on understanding what constitute typical policy violations from (Siponen et al. 2010)
  - Adapted 5 point Likert scales to 7 point scales
  - Demographic data: Gender, Age range, Department or Unit, Years of work, Educational background, and Type of employment

- Study procedures
  - Ethics from University of Strathclyde's Computer and Information Science Ethics Committee
  - Pilot Study
  - Paper based Questionnaires for non managerial staff with150 distributed, 115 returned of which 112 analysed and 3 discarded
  - All participants over 18 years and consented

Analysis & Results: Participant Demographics

		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)

		Participant Data	Organization Reality
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)

Despite some differences, we consider participants largely representative of the organization's employees

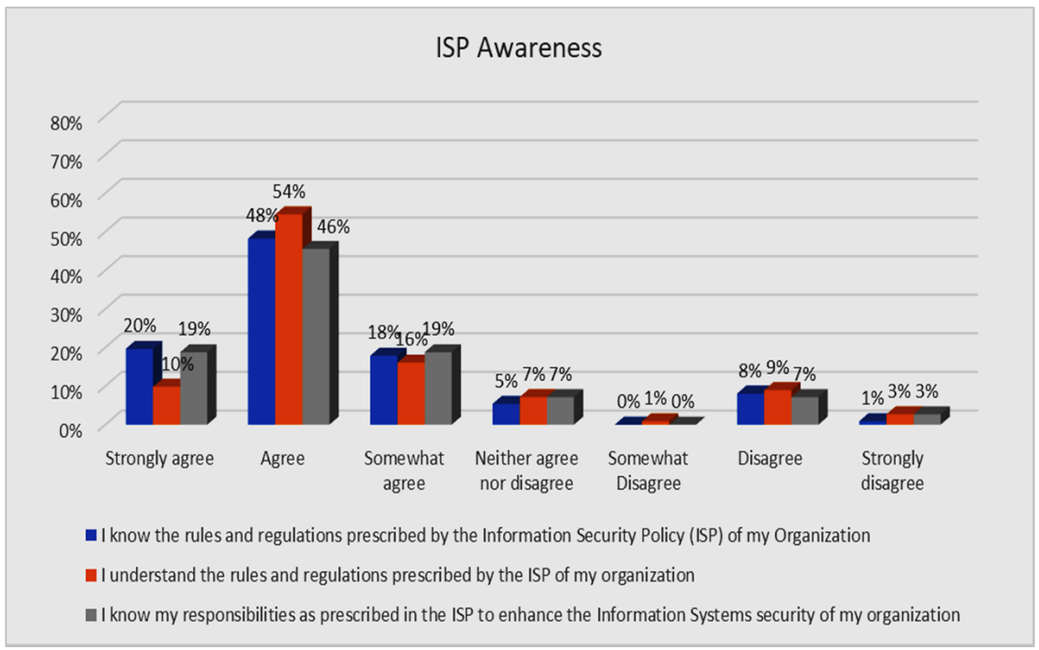
Analysis & Results: Reliability

- With Cronbach’s Alpha above 0.8 both scales are reliable

	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

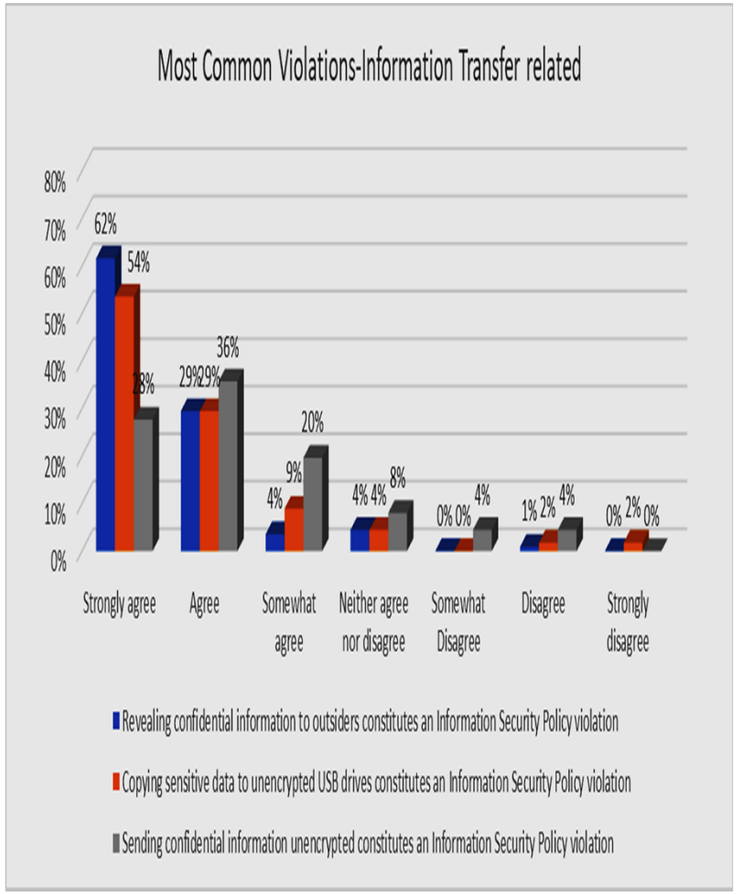
Analysis & Results: ISP Awareness

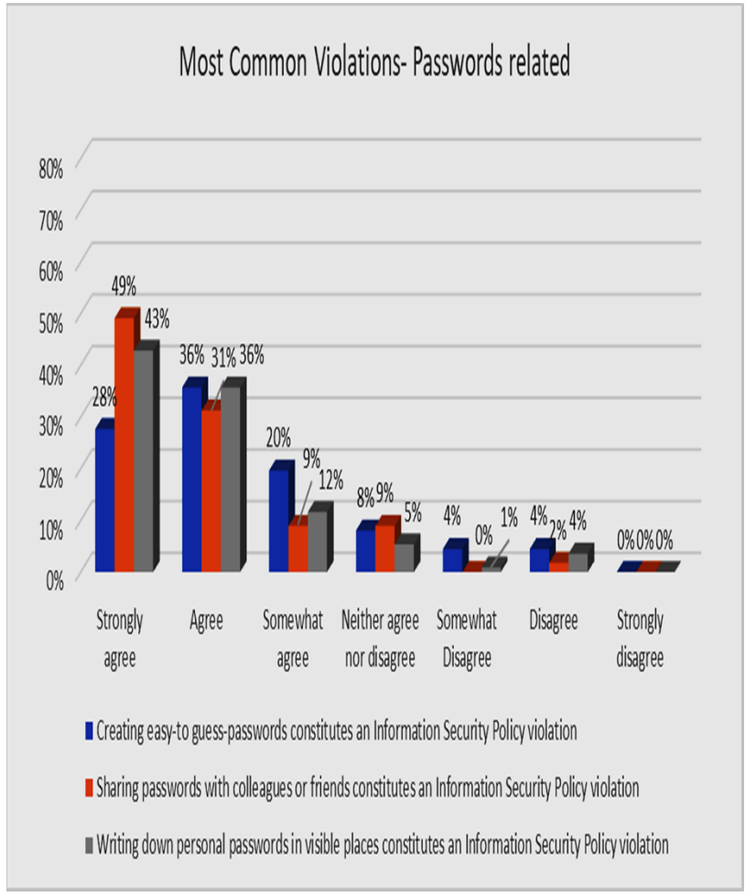
- Although most agree that they know (86%) and understand (80%) the provisions of the NIA ISP and know the responsibilities it prescribes (84%), some disagree
- However, there is no clear pattern in the characteristics of these participants that may explain their responses

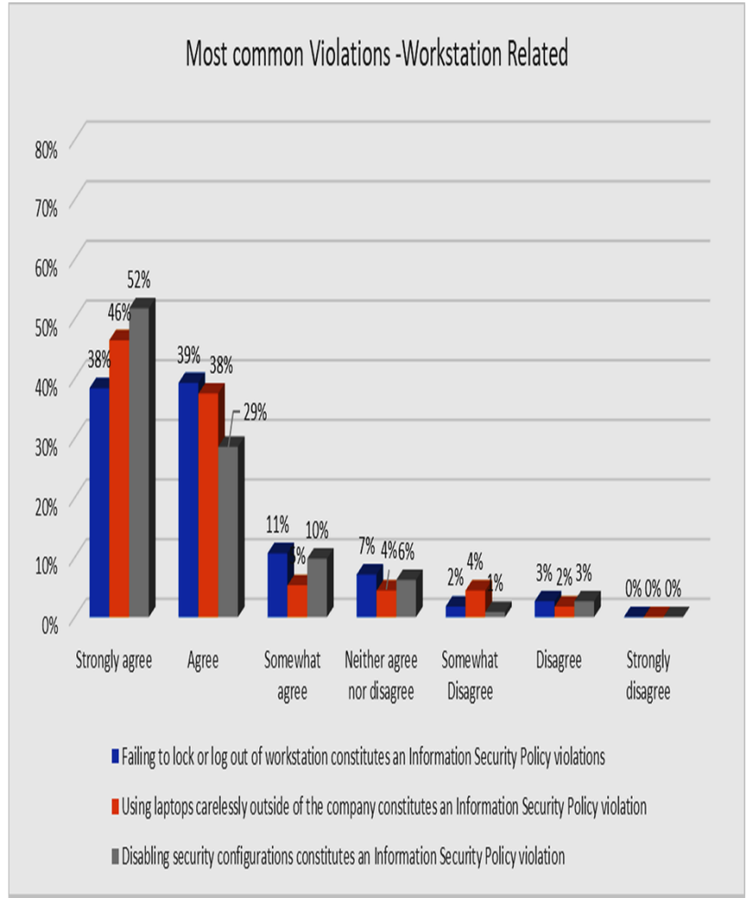


ISP Knowledge		
Gender	Experience	Count
Male	Experienced	1
Female	Experienced	4
	Inexperienced	4
ISP Understanding		
Gender	Experience	Count
Male	Inexperienced	2
Female	Experience	4
	Inexperienced	4
Knowledge of Responsibilities		
Gender	Experience	Count
Male	Experienced	1
	Inexperienced	1
Female	Experienced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

Analysis & Results: Most Common ISP Violations (1)







Analysis & Results: Most Common ISP Violations (2)

- Although 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, some disagree or are uncertain

- 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

Analysis & Results: Most Common ISP Violations (3)

	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

Analysis & Results: Most Common ISP Violations (4)

- 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 high-est standard deviations, 1.331 and 1.537 respectively, indicating the agreement to these constitute NIA ISP violation is not as strong as the rest

- Comparing the means and standard deviations of the common ISP violation questions to those of the awareness questions, the latter have higher means ranging from 2.46 to 2.72 and standard deviations between 1.381 and 1.490, indicating that agreement with the awareness questions is not as strong to the common ISP violations

Conclusion: NIA (1)

- 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 the NIA expects from them
- 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
- However. there is some room for improvement
  - Some differences in NIA staff agreement for certain violations are indicative of typical tensions between security and usability that staff training can help to address, see password selection
  - Other differences are indicative of lack of clarity that a formal ISP with coverage of bring-your-own-device expectations can help to address, see careless use of laptops
  - A combination of 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.

Conclusion: EIS (2)

- For EIS our research
  - Reinforces the need for a formal ISP for EIS that clearly specifies requirements for staff
  - Emphasizes the importance of staff training ensuring that policy provisions are fully appreciated and understood
  - Highlights the necessity to consider the organizational context in the development and implementation of the ISP

Study Limitations & Future Work

- Focus on staff of the NIA limits the generalizability of our findings
- Similar studies in other organizations and in other countries are necessary to generalize them

- A questionnaire based study limits the extent to which we can extrapolate from our findings the information security behaviours of NIA staff
- An observation study can establish whether staff behave in ways to prevent ISP violations

- Focus on NIA staff in non-management positions means management's views are not incorporated
- Surveying management views will address this

- Future work could also explore 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

- The covid 19 pandemic with government-imposed restrictions affected the period for the data collection
- Researchers may need to consider longer data collection periods to account for such unusual occurrences

Any Questions?

GRACIAS

University of
Strathclyde
Glasgow