INFORMATION SECURITY POLICY PERCEPTION VS REALITY

SALIM AWUDU
PhD Researcher, Department of Computer and Information Science

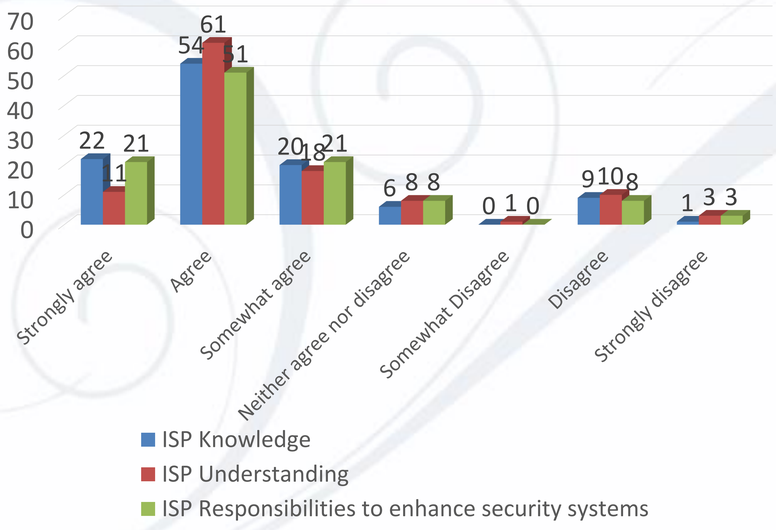
Introduction

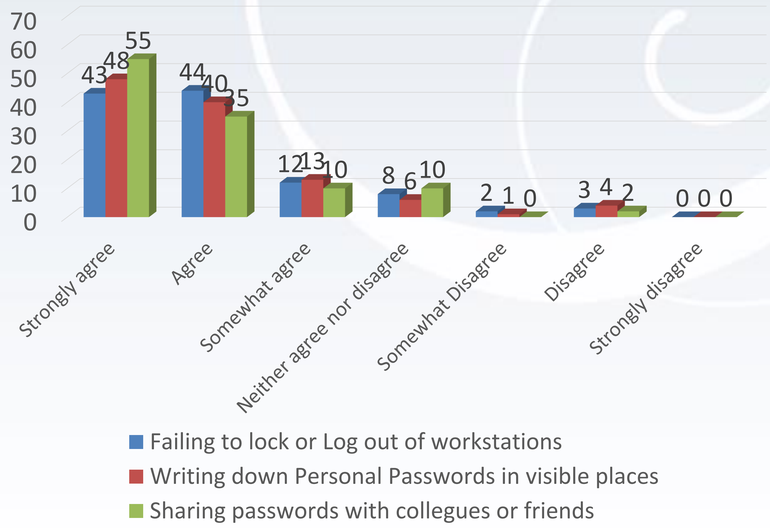
- Electronic Identity Systems (EIS) have become a tool to achieve economic, social and political development in many countries.
- However, organizations and individuals are concerned about EIS trustworthiness, privacy, and security.
- EIS require an effective Information Security Policy (ISP) underpinning technical, operational and managerial controls to address these concerns.
- The process through which the ISP is formulated, and the way it is expressed and implemented determines it effectiveness.
- However, it is not currently clear how to ensure the ISP of EIS should be formulated, expressed and implemented.
- To better understand what the requirements are, we conducted a survey at the Ghanaian National Identification Authority (NIA).

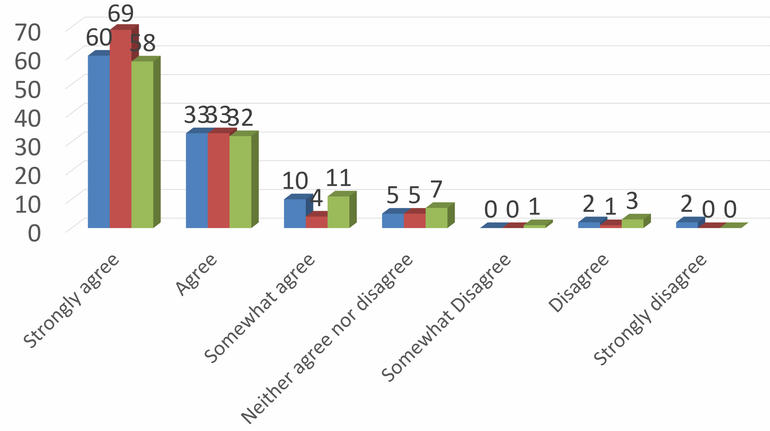
Study Design and Procedures

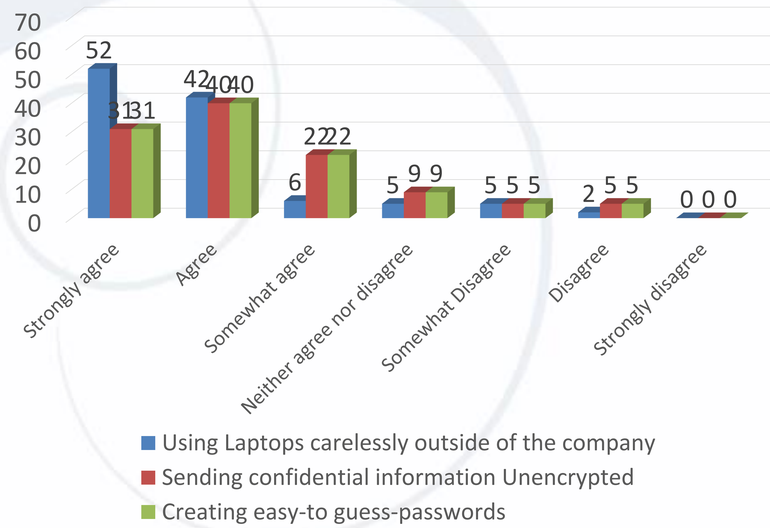
- Demographic questions on Gender, Age group, Education, Employment type, Years spent at NIA, Department/Unit and NIA Location.
- A set of 41 questions with 7-point Likert scale (Strongly Agree to Strongly Disagree) most of which were adapted from [1, 2].
- Study approval by Departmental Ethics Committee.
- Paper questionnaires distributed to 150 staff over a period of 8 weeks with 112 completed responses

Results









Conclusions

- NIA staff largely believe that they know and understand the provisions of the ISP and are aware of their obligations according to the ISP.
- However, there is a minority of staff that do not believe that to be the case across all 3 questions.
- Further analysis indicates that these are more experienced staff.
- This is potentially due to the informal approach followed by the NIA for its ISP in recent years in contrast to the past (provisions are communicated through notes rather than a formal policy document, and there is no formal training provided).
- A large majority of staff demonstrate their actual knowledge of the ISP provisions by agreeing that all 9 behaviours constitute ISP violations.
- However, their agreement is weaker for “Sending confidential information unencrypted” and “Creating easy-to-guess passwords”.
- This potentially indicates areas where more formal training may be required (staff may not really know how to effectively encrypt information and choose difficult to guess but easy to remember passwords)
- This potentially indicates also areas where the provisions of the ISP conflict with the operational reality (difficult to guess password can be difficult to remember, and encryption complicates the ability of employees to satisfy requests for information from government officials).

References

1. Siponen, M., & Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS quarterly, 487-502.
2. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 523-548.