Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol.4, No.8, 2014

Deepening the Knowledge on Information Security Management in Developing Countries: Evidence from Ghana

Kwabena Obiri-Yeboah[1*] Eliezer Ofori Odei-Lartey[2] Kwame Owusu Kwarteng[1]
1.Kwame Nkrumah University of Science and Technology, Kumasi, Ghana
2.Kintampo Health Research Centre, PO box 200, Kintampo-North, Ghana
* E-mail of the corresponding author: kyeboa@yahoo.com

Abstract
Following the seamless integration of the internet with computer information systems and the rapid increase in the number of people worldwide who possess the skills needed to launch cyber-attacks on public communication systems, businesses and organizations can hardly assume adequate security by depending on anonymity and geographical location. The basis of this study deepens knowledge on information security management in developing countries**.** This study uses both quantitative and qualitative approaches to examine the information security management practices of Social Security and National Trust in Ghana. Findings from results from the study suggest significant indications of human factor vulnerabilities and threats to information security. Findings also suggest that high levels of vulnerability to an external attack. Other findings however indicate management level recognition of education and training as very essential in improving information security practices. Although the results of this study may not be generalizable, we recommend that the issue of education and training on information security management should be made top priority on the IT agendas of all organizations in Ghana. A further study is proposed to assess the value placed on information security management within the context of developing countries and the factors that influence these values.
Keywords: Information Security Management, Cyber-attack, developing countries, computerization, security policy, security awareness, education and training

1. Introduction

Security risks in computerization have been extensively discussed in different studies. These studies identify causes of these risks ranging from errors by staff and deliberate act of sabotage, to natural disasters [1-3]. These risks are constantly being exploited by malicious individuals with varying reasons. Computer security attacks are increasingly becoming more complex. Following the seamless integration of network infrastructures and the internet with computer information systems and the rapid increase in the number of people worldwide who possess the skills needed to launch cyber-attacks on public communication systems [4], businesses and organizations can hardly assume adequate security by depending on anonymity and geographical location.

Management practices towards information security have important implications on effective use of information technology and successful development of information systems [5-7]. One major component of information security management is security policy availability and compliance [8, 9]. However, the commitment of management towards compliance to information security policy has very significant reflection on the information security management practices in an organisation [10-13]. The articulation of the rules rewards and punishment to business staff for compliance is also essential [14, 15].

Although the subject of information security management has been widely researched into, most literature focus on organizations in developed countries due to their known high dependency on information systems for advancement. Leveraging information technology for efficient management has become topical in Africa. This is evidenced by the increasing number of African research studies on the integration of computerized information systems into operations of public sector institutions; educational, financial and health sectors and businesses [16-20]. However, research into how these developing countries manage the security of information they collect, keep or share. The basis of this study therefore is to deepen the knowledge of information security management in developing countries.

In study, we examine the information security management practices of Social Security and National Trust (SSNIT) in Ghana. This study focuses on human factors and places emphasis on adherence and practice of information security practices at SSNIT.

The rest of this paper is in four sections. The first section is a review of the concepts of information security management. The second section is a description of the research methods used for the study. The results of the study is presented and discussed in the third section. In the final section of this paper, we conclude and outline recommendations based on findings.

2. Literature Review

The concept of information security (IS) is not contemporary. Information security practices date as far back as the 50 B.Cs, when Julius Caesar developed a shifted and substitution cipher system, to encrypt his military and government communications [21, 22]. Also in the 1790s, Thomas Jefferson created a 26 cipher wheel to propel messages from France to America when he was the Ambassador to France [22]. Thus during those times, Information security was a defense tool used by the military and government to hide confidential information. Information security sturdily permeated the business environment as competitive intelligence increased and various businesses sought to manage the protection of critical information that informed the core of their marketing and tactical strategies.

Earlier studies suggest that information security management (ISM) focused on protecting isolated infrastructure; computer systems, local area network systems, and data storage. Organizations frequently identified the potential threats and risks and provided a checklist to ensure [23-27].

In recent times, the internet has become an indispensable medium of information collection, storage and sharing for millions of organizations connected to it worldwide. Findings from a study indicated that as at 2008, sixty-eight per cent (68%) of large companies in Albania made use of online ordering facilities [28]. However, the numerous vulnerabilities of the internet make organisations prone to a host of possible attacks that compromise the confidentiality, integrity, and availability of information that they exchange through the internet. As a result a number of current ISM studies focuses on critical information exchange channels such as e-mail and e-commerce and cloud services [29-32].

Research studies suggest that the fundamental components of ISM are physical security of computer and network, security policy and security awareness [33-37]. Findings from these studies stress that security policy anchors the preceding three components on the basis that most of security decisions and practices in organisations are guided by management approved security policies. Thus, a security policy clearly defines the value and priority level of information assets in an organisation.

3. Data and Methods

This was conducted in August 2013. In this study, the exploratory design is adopted to understand information security management practices at the Social Security and National Insurance Trust (SSNIT). A survey strategy is employed to examine the research problem within the context of the case chosen.

The Trust has a total work force of about 2000 made up of casual and full time workers. Over fifty percent of these workers are computer users. The Trust has forty-nine (49) branches across the country; each of the branches is headed by a manager. There is also one IT personnel who heads the management information systems (MIS) department at each branch.

Workers of SSNIT are the population for this study. The selection of participants for this study is based on their roles as actors within the information distribution chain. The roles considered for this study are in two categories; those directly involved in information processing (common users) and those primarily responsible for information security management (IT heads and branch managers).

Results from this study are a reflection of the human factor rather than the technical equipment that manages the security of information assets. For this reason, study variables relate to attitudes, opinions and organizational practices.

Primary data for the study was collected through interviews and observational visits. Interactions with each of the participants under study consisted of a mix of closed-ended and open-ended questions. The questionnaires were either self-administered or interviewer-administered depending on the preference of the respondent. Self-administered questionnaires were physically delivered to and collected from the intended respondent to reduce possibilities of contamination and unknown biases

Though the sample is relatively small, diversity of the participants as well as the critical roles they play information management provides significant level of representativeness.

The total population of 2000 staff from the 49 branches of SSNIT across the country were grouped into 3 categories namely; Management, IT heads and computer Users. One hundred (90) participants were selected

from the population constituting 20 branch managers, 20 branch IT heads, and 50 computer users.

The data gathered is qualitatively analysed with the aid of SPSS.v20. In analysing, simple frequencies where used to show the distribution of participants in response to the interview questions. Pie charts and bar graphs are also used in the analysis to support the interpretation of the results

4. Results and Discussion

4.1 Characteristics of Respondents

In table 1, the characteristics of the respondents of the study are presented. Results in table two shows the characteristics of the respondents based on their involvement in the information distribution change and their level of influence on policy practices. The percentage proportions of responses relative to the total respondents are also presented. The total number of respondents (X) is reported as (N=X) at the header row.

Table 1: Summary Statistics on Characteristics of Respondents at SSNIT

Staff Category	**TOTAL NUMBER OF RESPONDENTS (N=90)**	
	n	**%**
Branch Managers	20	22.2
Branch IT Heads	20	22.2
Computer Users	50	55.6

Table 1 shows the characteristics of respondents to the study based on their level of involvement in influencing or managing information security.
The figures in the columns labeled 'n' for each panel show the observations for each response set. The figures in the columns labeled '%' for each panel show the proportions of each observation in percentage. The total number of respondents (X) for each response set is reported as (N=X) at the header rows for each panel.

In Table 1, results indicate three main classes of staff that have significant influence over the security of information at SSNIT; the branch managers, who oversee all activities at their respective branches and oversees the transmission of information across to branches; branch IT heads who are to ensure that the IT infrastructure at each branches are secure and fully functional; and lastly, common computer users who produce and transmit information both within and across branches.

4.2 Information Security Attacks and Threats

In Table 2, the characteristics of attacks and sources of security threats and vulnerabilities at SSNIT are presented. Results in Table 2 represent the attacks and sources of security threats based on responses received from the IT heads at SSNIT. The percentage proportions of responses relative to the total respondents are also presented. The total number of respondents (X) is reported as (N=X) at the header rows for each panel.

Table 2: Summary Statistics on Characteristics of Information Security Threats/Vulnerabilities at SSNIT

Panel A: Major Attacks	**RESPONSES FROM IT HEADS (N=20)**	
	n	**%**
Viruses	8	40.0
Unauthorized physical access	4	20.0
Network failure	8	40.0
Panel B: Major Sources of Threats and Vulnerabilities	**RESPONSES FROM IT HEADS (N=20)**	
	n	**%**
External Storage Media	3	15.0
Errors by users	8	40.0
Multiple sources	1	5.0
Negligence of users	8	40.0

Table 2 shows the characteristics of information security attacks, threats and vulnerabilities based on responses received from the interviewed IT heads. Panel A shows the major attacks reported by the IT heads interviewed. Panel B shows the major sources of threats and vulnerabilities as reported by the IT heads interviewed. The figures in the columns labeled 'n' for each panel show the observations for each response set. The figures in the

columns labeled '%' for each panel show the proportions of each observation in percentage. The total number of respondents (X) for each response set is reported as (N=X) at the header rows for each panel.

In Table 2, results from Panel A show that the major attacks are viruses (40%) and network failures (40%). The results from Panel A further indicate evidence of unauthorized physical access (20%) to restricted areas. Results from panel B also indicates that, user errors (40%) and negligence (40%) rank top on the sources of virus attacks and network failures. Results from Table 2 confirm the literature findings that the most vulnerable source of threats to any security attack is the human component.

Following the evidence of unauthorized physical access to restricted information areas, we further present results on reported cases of unauthorized entries from the Headquarters and two other branches of SSNIT within five working days in Table 3. The figures in table one, for each day, are separated into access by unauthorized staff (S) and unauthorized non-staff or visitors (V).

Table 3: Summary Statistics on Unauthorized Physical Access from three SSNIT Branches in Five Working Days

Unauthorized entries at three SSNIT branches	**DAY 1**		**DAY 2**		**DAY 3**		**DAY 4**		**DAY 5**		**TOTALS**		
	S	**V**	**S**	**V**	**S**	**V**	**S**	**V**	**S**	**V**	**TS**	**TV**	**Total**
Headquarters	20	4	15	2	35	1	16	7	10	12	96	26	122
Adum	8	0	10	0	13	0	7	5	9	13	47	18	65
Asafo	13	0	6	4	12	1	17	0	4	10	52	15	67

Table 3 shows statistics of reported cases of unauthorized physical access to restricted information areas within five working days. The header labels 'DAY 1' through to 'DAY 5' is the five working days observed within one week. The columns labeled 'S' in Table 3 show the figures for unauthorized access by SSNIT staff. The columns labeled 'V' show the figures for unauthorized access by non-staff or visitors. The columns labeled 'TS' and 'TV' show the total number of unauthorized access by staff and visitors respectively. The column labeled 'Total' presents the overall total for each of the three branches of SSNI .The first row in Table 3 shows unauthorized access at the SSNIT headquarters. The second and third rows show unauthorized access at Adum and Asafo branches of SSNIT respectively.

Results from Table 3 suggest a relatively high level of unauthorized access is experienced at the headquarters. Results further suggest that access restriction is mainly violated by staff of SSNIT. The results also indicate an increase in the number of unauthorized visitor access over staff access on the fifth working day. Moreover, the total number of unauthorized physical access by visitors for the five working days is significant. It is expected that an attack would usually be from within an organisation [38] but results from Table 3 suggests that SSNIT may be highly vulnerable to information security breaches from a non-staff. One major reason given for access violations by visitors was that staffs in such restricted offices do not have a room where they could receive their visitors; both personal and official.

4.3 Information Security Management Practices

In Table 4, results on management orientation towards information security management practices at SSNIT are presented. The results presented are based on responses received from branch IT professionals. Results in Panel A represent the Awareness of the branch IT professionals about the availability of a policy document. In Table 4, Panels B, C and D present results on how the branch IT professionals manage information security. Finally, Panel E presents results on suggested budget commitment to information security management at SSNIT from the perspective of the branch IT professionals.

Table 4: Summary Statistics on the Orientation IT Professionals towards ISM Practices

Panel A: Awareness about the Availability of ISM policy document	**RESPONSES FROM IT PROFESSIONALS (N=20)**	
	n	**%**
Yes	13	65.0
No	0	0.0
I don't know	7	35.0
Panel B: Practice of ISM principles	**RESPONSES FROM IT PROFESSIONALS (N=20)**	
	n	**%**
Access restriction and out-of-bounds labels on door posts	16	80.0
Password Enforcement and Encryption of data	12	60.0
Rewards and Punishment for policy compliance	13	65.0
Panel C: Implementation of security measures	**RESPONSES FROM IT PROFESSIONALS (N=20)**	
	n	**%**
Biometric / electronic door locks	13	65.0
CCTV	1	5.0
Panel D: Disposing off worn-out computers	**RESPONSES FROM IT PROFESSIONALS (N=20)**	
	n	**%**
Donation	7	35.0
Sent back to stores	6	30.0
Auctioned	4	20.0
Destroyed	0	0.0
Don't know	5	25.0
Panel E: Budget commitment to ISM	**RESPONSES FROM IT PROFESSIONALS (N=20)**	
	n	**%**
1 – 5%	9	45.0
6 – 10%	4	20.0
11 – 15%	5	25.0
16 – 20%	1	5.0
I don't know	1	5.0

Table 4 shows summary statistics on the awareness, practices and suggested budget commitment by IT professionals to information security management policies at SSNIT. The figures presented are based on responses from the IT professionals. Panel A shows responses on the awareness of the availability of an information security management policy document. Panels B and C indicate the policy guidelines that are enforced as well as other security measures that are implemented by the IT professionals. Panel D shows responses on practices of disposing of worn-out computers at SSNIT. Panel E shows responses on suggested budget commitment to information security management. The figures in the columns labeled 'n' for each panel show the observations for each response. The figures in the columns labeled '%' for each panel show the proportions of each observation in percentage. The total number of respondents (X) for each study area is reported as (N=X) at the header rows for each panel.

Results in Table 4 suggest that a significant proportion of IT professional (35%) are not sure about the availability of an ISM policy document, despite their fundamental roles as IT heads and experts at the various branches of SSNIT they operate from. This awareness deficit may have an association with the shortfalls in ISM practices as shown in panel B and C of Table 4. Moreover varied responses were given on how computers are disposed when warn out as well as suggested budget commitments. Laxity on the part of management in ISM policy compliance is reflected in the responses given by the IT professionals who are primarily responsible for the safeguard of the Trust's information assets.

We further examine ISM from responses received from the lay users interviewed concerning ISM at SSNIT. In

Table 5, results in panel A indicate the distribution for users who confirmed that they have been assigned a specific user account. Panel B shows the distribution for users who have places passwords on their user account. Panel C indicates frequency at which users change their passwords. Panel E also shows the distribution for users who give their passwords out to allow others to access their accounts. Results in panel E indicate the number of users who frequently update their antivirus signatures. Panels F and G indicate users who have restrictions on installing a new program or browsing any website in the internet. Panel H shows concerns raised by lay users on practices that negatively affect ISM.

Table 5: Summary statistics on the Orientation of Lay Users towards ISM Practices

Panel A: Assignment of User accounts to Lay Users	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	40	80.0
No	10	20.0
Panel B: Lay Users with Password-enabled account	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	38	76.0
No	12	24.0
Panel C: Frequent Change of Password by Lay User	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Monthly	2	4.0
Quarterly	9	18.0
Twice a year	5	10.0
As and when necessary	20	40.0
Never	2	4.0
Not Applicable	12	20.0
Panel D: Voluntary password sharing by Lay User	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	28	56.0
No	10	20.0
Not Applicable	12	24.0
Panel E: Lay User Self-update of Antivirus Signatures	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	14	28.0
No	36	72.0
Panel F: Lay User Unrestricted Installation of programs	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	6	12.0
No	44	88.0
Panel G: Lay User access to Unlimited Internet Websites	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Yes	14	28.0
No	36	72.0
Pane H: Information Security concerns raised by Lay Users	**RESPONSES FROM LAY USERS (N=50)**	
	n	**%**
Unlimited/ unrestricted access	7	14.0
Use of strange devices on the PC	2	4.0
Frequent breakdowns of computers	7	14.0
Storage challenges	2	4.0

Table 5 shows summary statistics on lay user responses that reflect ISM practices at SSNIT. Panel B shows the distribution for users who have places passwords on their user account. Panel C indicates frequency at which users change their passwords. Panel E also shows the distribution for users who give their passwords out to allow others to access their accounts. Results in panel E indicate the number of users who frequently update their antivirus signatures. Panels F and G indicate users who have restrictions on installing a new program or browsing any website in the internet. The figures in the columns labeled 'n' for each panel show the observations for each response. The figures in the columns labeled '%' for each panel show the proportions of each observation in percentage. The total number of respondents (X) for each study area is reported as (N=X) at the header rows for each panel.

In Table 5, results indicate that a high number (40/50) of lay users have been assigned specific user accounts. Results further indicate that most (38/40) of the users with specific user accounts use passwords to protect their accounts. However, results in panel C suggest that less than half (15/38) of the users with passwords on their user accounts have scheduled times for changing passwords. Also, results in panel D indicates that a very high number of lay users with user account allow others to user their accounts by giving out their passwords.

Results on updates of antivirus signatures in Table 5 indicate that most lay users (36/50) do not ensure that their antivirus signatures are up-to-date. However, some of these lay users (6/50) are not restricted on the programs they are able to install on their computers as well as the internet websites (14/50).
Results in Table 5 further indicate that lay users have raised security concerns about unlimited access (7/50), the use of unknown removable devices by other users (2/50). Other challenges raised by these lay users include the frequent breakdown of the computers they are using (7/50) as well as the unavailability of storage space (2/50).

We further solicit views from IT professionals and branch managers to improve ISM as presented in Table 6. In table 6, Panel A shows suggestions from IT professionals about the improvement of ISM whiles panel B shows suggestions from branch managers of ways to improve ISM practices.

Table 6: Summary Statistics on Suggestions for Improving ISM Practices

Panel A: Suggestions by IT Professionals to improve ISM	**RESPONSES (N=20)**	
	n	**%**
Provide CCTV cameras	2	10.0
Acquisition of a Strong Antivirus	3	15.0
Management Commitment to Policy Compliance	3	15.0
Information Security Awareness Training	10	50.0
Panel B: Suggestions by Branch Managers to improve ISM	**RESPONSES (N=20)**	
	n	**%**
Frequent change of password	2	10.0
User opinion should be sought	1	5.0
Staff within should do the maintenance	2	10.0
Regular training of both the professionals and the non-professionals	10	50.0
IT department should be created	1	5.0

Table 6 shows results on views solicited from IT professionals and branch managers of SSNIT on ways to improve ISM, Panel A shows suggestions from IT professionals about the improvement of ISM whiles panel B shows suggestions from branch managers of ways to improve ISM practices. The figures in the columns labeled 'n' for each panel show the observations for each response. The figures in the columns labeled '%' for each panel show the proportions of each observation in percentage. The total number of respondents (X) for each study area is reported as (N=X) at the header rows for each panel.

From Table 6, suggestions to improve ISM by IT professions include the provision of more security cameras, the acquisition of a strong antivirus program, improved commitment of management to ISM policy compliance and Educating staff on best practices of information security. The education of staff on information security was suggested by a high number of respondents (10/20).

From the perspective of managers, training also stood out (10/20) among other suggestions for improvement. There was also a suggestion that an IT department should be created at every SSNIT branch to independently manage information security

5. Conclusion

Leveraging information technology for good governance and public administration has become a topical in African countries. However, research into how these developing countries manage the security of information they collect, keep or share. The basis of this study therefore is to deepen the knowledge of information security management in developing countries.

In study, we examine the information security management practices of Social Security and National Trust (SSNIT) in Ghana. This study focuses on human factors and places emphasis on adherence to information security practices at SSNIT. Primary data for the study was collected through interviews and observational visits. Interactions with 90 participants under study consisted of a mix of closed-ended and open-ended questions. Though the sample is relatively small, diversity of the participants as well as the critical roles they play information management provides significant level of representativeness

Results from the study suggest that there may be high human factor vulnerabilities and threats to information security at SSNIT. Results also suggest that SSNIT may be highly vulnerable to an external attack, considering the number of visitors that have unauthorized access to restricted areas. Results from the study further suggest that security policies are barely enforced, which is evidence by the weak level of adherence and culture of information security practices by lay users. Results also suggest that the management of SSNIT see education and training to be very essential in improving information security management.

Following the forgoing findings, the issue of education and training on information security management should be made top priority on the IT agendas of SSNIT. The issues of budget and other commitments to information security by management should however not be under emphasized.

The results of the study may not generalizable to all organizations in developing countries given the relatively small sample size; it rather provides an initial platform for an understanding of information security practices in developing countries and sheds light on the requirements for good information security implementation.

Results from this study are oriented towards the opinions of respondents rather than statistical indices which may have provided more indicative results that link ISM practices to measured outputs and benefits. Further studies may also assess value placed on information security management within the context of developing countries and the factors that influence these values.

REFERENCES

1. Abu-Musa, A.A., *Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry.* Journal of Information Systems, 2006. **20**(1): p. 187-203.
2. Sumner, M., *Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness.* Information Systems Management, 2009. **26**(1): p. 2-12.
3. Whitman, M.E., *In defense of the realm: understanding the threats to information security.* International Journal of Information Managment, 2004. **24**(1).
4. Choo, K.-K.R., *The cyber threat landscape: Challenges and future research directions.* Computers & Security, 2011. **30**(8): p. 719-731.
5. Gunasekaran, A. and E.W.T. Ngai, *Information systems in supply chain integration and management.* European Journal of Operational Research, 2004. **159**(2): p. 269-295.
6. Niederman, F., J.C. Brancheau, and J.C. Wetherbe, *Information systems management issues for the 1990s.* MIS Q., 1991. **15**(4): p. 475-500.
7. Alavi, M. and D.E. Leidner, *Knowledge management systems: issues, challenges, and benefits.* Commun. AIS, 1999. **1**(2es): p. 1.
8. Herath, T. and H.R. Rao, *Protection motivation and deterrence: a framework for security policy compliance in organisations.* European Journal of Operational Research, 2009. **18**(2): p. 106-125.
9. Vroom, C. and R. von Solms, *Towards information security behavioural compliance.* Computers & Security, 2004. **23**(3): p. 191-198.
10. Pahnila, S., M. Siponen, and A. Mahmood. *Employees' Behavior towards IS Security Policy Compliance*. in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. 2007.
11. von Solms, S.H., *Information Security Governance – Compliance management vs operational management.* Computers & Security, 2005. **24**(6): p. 443-447.
12. von Solms, B. and R. von Solms, *The 10 deadly sins of information security management.* Computers & Security, 2004. **23**(5): p. 371-376.
13. Dutta, A. and K. McCrohan, *Management's Role in Information Security in a Cyber Economy.* California Management Review, 2002. **45**(1).
14. Ryu, S.-H., D.-R. Jeong, and H.-K. Jung, *Ways to establish public authorities information security governance utilizing E-government information security management system (G-ISMS).* Journal of the Korea Institute of Information and Communication Engineering, 2013. **17**(4): p. 769-774.
15. Kyle Kallender, P., *Waking Up to a New Threat: Cyber Threats and Space.* TRANSACTIONS OF THE JAPAN SOCIETY FOR AERONAUTICAL AND SPACE SCIENCES, AEROSPACE TECHNOLOGY

JAPAN, 2014. **12**(ists29): p. Tv_1-Tv_10.
16. Snyders, F. and L. Van Dyk, *Developing Business Models for Using Mobile Phones to Strengthen Preventative Healthcare in South Africa*. 2014. Vol. 2. 2014.
17. Diedericks, E. and S. Rothmann (2014) *Flourishing of information technology professionals : effects on individual and organisational outcomes*. **45**, 27-41.
18. Naidoo, V. and B. Van Niekerk (2014) *Strategic information security management as a key tool in enhancing competitive advantage in South Africa*. **11**, 33-46.
19. Pretorius, H., A. Leonard, and I. Strydom (2013) *Towards an electronic monitoring, observation and compliance framework for corporate governance using business process management systems : building the information society*. 62-75.
20. Obiri-Yeboah, K., W. Owusu-Ansah, and E.O. Odei-Lartey, *Factors that Drive Internet Usage among Small and Medium Scale Enterprises: Evidence from Ghana.* International Journal of Management & Marketing Research, 2013. **6**(2): p. 17.
21. Krause, M. and H.F. Tipton, *Information Security Managment Handbook*. 2004, CRC Press LLC.
22. Whitman, M.E. and H.J. Mattord, *Cryptography*, in *Principles of Information Security*. 2011, Cengage Learning. p. 351.
23. Goldwasser, S., S. Micali, and R. Rivest, *A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks.* SIAM Journal on Computing, 1988. **17**(2): p. 281-308.
24. Kwok, L.-f. and D. Longley, *Code of Practice: A Standard for Information Security Management*, in *Information Security in Research and Business*, L. Yngström and J. Carlsen, Editors. 1997, Springer US. p. 78-90.
25. Schweitzer, J.A., *Securing Information on a Network of Computers.* EDPACS, 1987. **15**(1): p. 1-8.
26. von solms, R., et al., *A framework for information security evaluation.* Information & Managment, 1994. **26**(3): p. 143-153.
27. Wood, C.C., *Establishing internal technical systems security standards.* Computers & Security, 1986. **5**(3): p. 193-200.
28. BAHITI, R., *ICT IN SMALL AND MEDIUM ENTERPRISES (CASE OF ALBANIA).* EPOKA UNIVERSITY CENTER FOR EUROPEAN STUDIES, 2008: p. 184.
29. Bacon, J., et al., *Information Flow Control for secure cloud computing.* 2014.
30. Demirkan, H. and J. Spohrer, *Developing a framework to improve virtual shopping in digital malls with intelligent self-service systems.* Journal of Retailing and Consumer Services, 2014.
31. Hartono, E., et al., *Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation.* Decision Support Systems, 2014.
32. Riquelme, I.P. and S. Román, *Is the influence of privacy and security on online trust the same for all type of consumers?* Electronic Markets, 2014: p. 1-15.
33. De, S.J. and A.K. Pal. *A Policy-Based Security Framework for Storage and Computation on Enterprise Data in the Cloud*. in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*. 2014.
34. Mishra, S., et al., *The Role Of Awareness And Communications In Information Security Management: A Health Care Information Systems Perspective.* International Journal of Management & Information Systems (IJMIS), 2014. **18**(2): p. 139-148.
35. Slocombe, G., *Cyber security: Defence information assurance.* 2014.
36. Bulgurcu, B., H. Cavusoglu, and I. Benbasat, *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.* MIS quarterly, 2010. **34**(3).
37. Denning, D.E.R., *Information warfare and security*. Vol. 4. 1999: Addison-Wesley Reading MA.
38. Colwill, C., *Human factors in information security: The insider threat–Who can you trust these days?* Information security technical report, 2009. **14**(4): p. 186-196.

BIOGRAPHY

Kwabena Obiri-Yeboah is a lecturer in Information Systems at Kwame Nkrumah University of Science and Technology (KNUST), Ghana. He had his MSc in Management Information Systems from University of Texas at Dallas. He has 12 year experience in IT systems development; 10 years with JCPenney Corporation in Dallas. His areas of interest include IT adoption in business, IT policy and IT education. He can be contacted at: Department of Decision Science, KNUST School of Business, KNUST, Kumasi-Ghana. Phone: +233241076524. Email: kobiri-yeboah.ksb@knust.edu.gh or kyeboa@yahoo.com

Eliezer Ofori Odei-Lartey is a Data Manager and a Research Fellow at the Kintampo Health Research Centre. He holds an MBA in Business Information Technology from the Kwame Nkrumah University of Science and Technology (KNUST). He can be contacted at: Kintampo Health Research Centre, P. O. Box 200, Kintampo-North, Brong Ahafo Region - Ghana. Phone: +233246926396. Email: eliezer.lartey@kintampo-hrc.org or elelart@gmail.com

Kwame Owusu Kwarteng is a lecturer in Informatics at Kwame Nkrumah University of Science and Technology (KNUST), Ghana. He holds an MBA in Business Information Technology from the Kwame Nkrumah University of Science and Technology (KNUST). His areas of interest include IT adoption in business, IT in small and medium enterprises and IT education. He can be contacted at: Department of Decision Science, KNUST School of Business, KNUST, Kumasi-Ghana. Phone: +233203288888. Email: kowusukwateng@yahoo.com

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar