The Imperative Information Security Management System Measures In the Public Sectors of Ghana. A Case Study of the Ghana Audit Service

Dr Ing Edward Opoku-Mensah,
Lecturer, Department of ITE, University of Education, Kumasi, Ghana.

Christopher A Abilimi,
Lecturer, Computer Science Department, Christian Service University College, Ghana.

Linda Amoako,
Lecturer, Computer Science Department, Christian Service University College, Kumasi, Ghana.

ABSTRACT

The essence of information usage in the public sectors of Ghana is very important as these sectors usually keep information about citizens as well as their clients. It is important that measures and tools are put in place to manage such information and ensure its security. The researchers investigated the various security breaches and recommended measures to overcome or manage the breaches. A survey was carried out on Ghana Audit Service using purposive sampling for sampling various stake holders involved in the audit sector. The results were analysed using the statistical software SPSS (Statistical Package for Social Sciences) and presented in tables and figures and the necessary parameters discussed.

Keywords Information Technology, Ghana Audit Service, Information Security Management.

Introduction

The Iran National Standard (2007) revealed that about 60% of firms around the world have shown that security-related problems are not easy for them and about seventy-second percentile of companies have shown the anxiety of information security of their property as well as the physical security of their possessions and how these are very important to them. In the area of public and private sectors of different kinds of companies there is the presence of undesirable conditions when it is about the security of information exchange (Abrar News, 2013). Accordingly so many companies in different countries across the world have tried to address the problems associated with the management of information security systems. Very few companies have received information security certificates. In Ghana for example it is doubtful if any company has this certificate, and the total number of companies worldwide that have obtained the information security management certificate is now seven thousand two hundred and five (Chamanzamin & Rezvani, 2004). However it is gratifying to note that the number of organizations accessing the certificate keeps growing, thus indicating how pertinent information security is to both public and private organisations. Stanton et al. (2005) pointed out four main directions related to information security: The user interfaces of information security management concerns relating to finances of the business process, security-related systems, managerial problems regarding harmful computer usage and information security behaviour .

The security of information in various sectors across the world, whether municipal or metropolitan, is both vital and crucial. Unfortunately, such vital pieces of information are stored in databases. The problem of sudden data loss and unlawful access of companies' information is reduced when better measures are used and implemented for the protection of data. This paper takes a look at the factors of information security management system successful in the public sector, from the perspective of the Audit Service of Ghana, particularly called Ghana Audit service (GAS). It is with this background that the researchers investigated the concern of information security for the GAS, and all others public sectors for that matter, for the protection of public resources.

Information Security Management in the Public Sector

According to Solms et al. (2000), the protection and information asset security in firms' framework where information system is running using a sequence of administration actions is called Information

Security Management. There are diverse ways by which different firms' information property can be evaluated and reasons for the difference could be both business areas as well as geographical locations of the company. That means that companies located in developing countries that have poor organizational development may not pay much attention to protecting their secret information while their counterparts in the developed countries that have good organizational development may pay more attention to protecting their information assets. The paramount aim is to reduce the problem that an information asset encounters (Solms et al., 2000). Table 1 below shows an effectual information security management system as postulated by Nosworthy in 2000.

Table 1:The determinants of a successful information security management system

Determinants	Explanation of of Determinants
Humans beings	Various events can be caused by People. Without Human beings Information security policy has no meaning
Culture of the society	Information security management is associated with managerial culture and is very crucial in protecting confidential data. The plans for different information security systems are different. For example Information security management plan that is used for a service company is different from that of a manufacturing plant.
Mind-set of humans beings	How people look at the security of a company and what it means to the company is the different approach to information security by humans.
Security education	All qualified staff needs adequate education so that they can implement various information security management plans to their diverse firms.
Work description of individuals	Various work distributions should identify individual roles in the areas of training, information security and documentation.

Source: Nosworthy, J. (2000).

The public sector, which is often fragmented and subject to competing and sometimes conflicting mandates, faces special challenges in managing the flow and security of information. For public sector to effectively meet its obligations to provide national security, public safety and accessible services to people in terms of information, the sector must overcome the constraints of bureaucracy and build stronger mechanisms to protect information by adopting these successful factors proposed by Nosworthy (2000), and taking human, culture, attitudes, security and job description into consideration.

Challenges of Information Security in the Public Sector

Cloud computing enables information sharing to be the much talked about subject in today’s computing or information technology. The much scalable, flexible and powerful computing is enabled by cloud computing as seen by the civil sectors of the world. On the other hand, cloud computing, raises many security problems from its model and there is no obvious explanation to issues such as access, once the information leaves the multitude business, compliance and data security. In public sector, many standards of software and hardware create considerable issues in terms of security, in terms of data processing, storage and retrieval. Every stakeholder in healthcare organization should have enough information security education, and sufficient knowledge to understand the potential vulnerabilities, which exist in a system versus either insiders or outsiders (Åhlfeldt, 2001). Every day a number of public sector records are created. Government highly depends on this information for decision making. Therefore, there should be appropriate and well-organized procedures and standards to store, manage and secure such information to ensure confidentiality, integrity and availability. Information and Communication Technology (ICT) has contributed both positively and negatively as threats to information, as its application increases in rhythm technological advancements. Again, the sharing of information is a big security risk, and therefore, the flow of such information among stakeholders needs to be secure and reliable in terms of confidentiality and integrity in order to ensure acceptable information for the user. Information security officers are a key part of the migration to the cloud and have serious concerns about cloud computing. Basic information security challenge in public sector can be threats, risk, crimes and access control issues. As asserted by Frost and Sullivan (2011), public sectors believe that the exposures of confidential or sensitive information, data loss, or leaks are of greatest concern to them. Compared to other challenges in the sector, cloud computing is one area in particular where information security officers cited the need for additional training and new skills. The skills that officers indicated as necessary for information sharing are different from traditional security skills **(**Frost & Sullivan, 2011). This has been echoed by Mahmood and Ashrafullah (2010) that, most of public sector information users have inadequate security training, insufficient security education, and lack of knowledge and unawareness of technical security, which can lead to more error.

There is a disturbing increase in information insecurity in the public sector corroborated by the fact that the character of the information public sector requirements for the sector under the Freedom of Information Act, showed that public sectors have to lead the campaign for high standards of information management records (Keans, nd). Rent research from Shred-it and File stores showed that one in three (34%) public sector organisations have experience of employees leaking confidential information from inside their organisations. Sensitive information of public sector stands the risk of being transformed and translated among various actors in Ghana, and this electronic public sector information becomes more vulnerable due to distribution of information, and deficiencies both at technical and administrative levels.

Methodology

Sample Size and Sample Procedure.

The research was a case study of the Ghana Audit Service. Purposive sampling technique was used for selecting the Ghana Audit Service (GAS), Kumasi, as representative sample of the entire GAS. This sampling technique was adopted as the most suitable for answering the research question(s) and for meeting the objectives as asserted by Saunders et al. (2009). Purposive sampling was also used because, according to Saunders et al. (2009), this sample is often used when working with very small samples such as the case of GAS in Kumasi. The total population of GAS in Kumasi was one hundred (100), and since the entire staff was reachable all the staff was included in the study. The total staff at GAS Kumasi was ten (10) IT Officers, seventy-five (75) staff in the districts and fifteen (15) administrative staff. The use of the whole population was also meant to increase the validity and reliability of the study and make the outcome of the study more representative of the total population of the Ghana Audit Service.

Data Collection Instrument and Procedure

Questionnaire and interview were used as the tools for obtaining the necessary information for the research. Structured questionnaire and semi-structured questionnaire were developed by the researchers and administered to respondents one by one. The questionnaire was made up of open-ended and closed-ended items. The questionnaire was divided into three parts. Part one included IT Policies at Ghana Audit Service. Part two was made of the factors and challenges of information security at Ghana Audit Service and the third part dealt with the importance of information security at Ghana Audit Service. The heads of departments were also interviewed. The interviews took the form of conversation in which respondents were asked questions in connection with the research topic. The researchers used that opportunity to throw more light on the research objectives. Also the interview technique made way for effective use of feedback, which enhanced the clarification of any arising issues.

Data Analysis

The nature of the study required both qualitative and quantitative analysis of data gathered. In this study, most of the cases were rated on a point scale for instance a scale of 5 was assigned to very high and 1 to very low. Data collected were analyzed and summarized into statistical tables and charts to make interpretation easier with the help of statistical package for social sciences (SPSS). The following are the presentation and analysis of the various security policies of Ghana Audit Service (GAS) on Information Security (IS) as revealed by the study:

Training on Information Security (IS)

Figure 1 below answers the question **“**Have you received any education in information security?” This question was meant to find out if the respondents had education on information security. This would help them to appreciate the importance of information service and address its challenges.

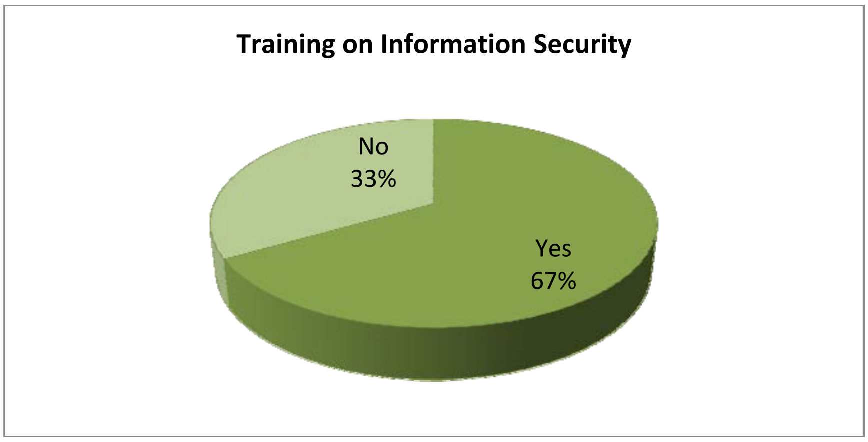

Figure1: Training on Information Security (IS)
(Source: Author’s field study, 2013)

Figure1 shows that, majority of the respondents representing 67% had some training in information security whiles one out of three of them (33%) had no education in IS. This revelation that as much as 33% of employees lacked any education in information security was not healthy and could be a challenge to the operations of the organization. The reason was attributable mainly to lack of funds and also for the fact that training programs, if any, were centralised and done at head office.

Potential Challenges to GAS Information

Figure 2 below answers the question “is information at GAS exposed to any potential challenge?” This question was meant to determine if there was any additional challenge of IS that was not captured in the literature review but happens at GAS.

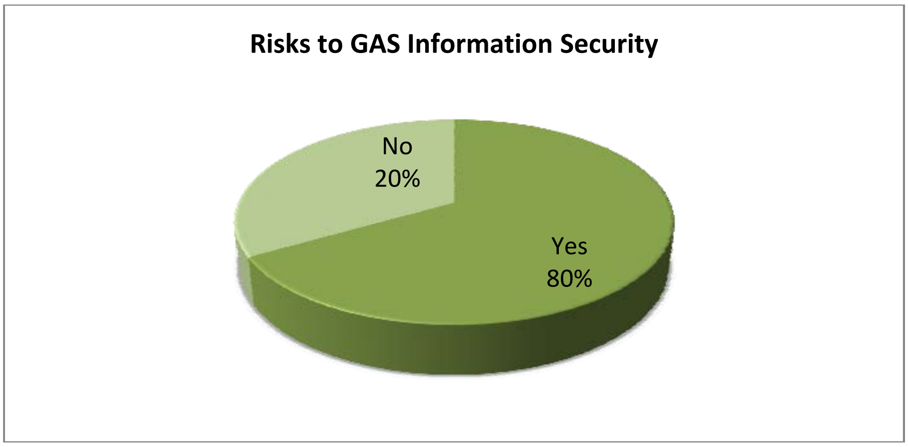

Figure 2: Risks to GAS Information Security
(Source: Author’s field study, 2013)

Figure 2 indicates that, majority (80%) of the respondents agreed that, there were information security challenges at Ghana Audit Service while few (20%) of the respondents said there were no potential

information security challenges at Ghana Audit Service. These challenges were confirmed below by respondents.

Additional Challenges at Ghana Audit Service

The following are the additional factors that were listed by the respondents as challenges of IS at GAS:

- Inadequate education on information security at GAS. The level of education on IS for personnel to appreciate the importance of it was not adequate.
- Antivirus software was not updated as frequent as expected. This leads to machines being affected by viruses, Trojans and worms.
- Many of the personnel did not know how to secure information. This makes protecting confidentiality and integrity very difficult to achieve.
- Frequent lock up of computers requiring administrative assistance. This raises a concern and supports the assertion that, personnel did not know much about computing and information security.
- Documents were most often not “protected”. This means that any intruder or visitor could have access to documents thereby compromising their integrity.

Challenges of Information Security at GAS

Table 2 answers the question “how will you rate the following as a challenge of information security at GAS?” This question was meant to determine the challenges GAS was exposed to.

The responses of the respondents were measured on a 5-point Likert type rating scale. The arithmetic mean and standard deviations were also calculated to analyse the responses. The responses from the interview with key staff listed many challenges of information security at GAS. Their responses were compared with the questionnaire to assess their views and ensure validity and reliability.

Table 2: Challenges of Information Security at GAS

Challenges of Information Security at GAS	**N**	**Mean**	**Std. Deviation**
Data security	100	4.14	.95
Compliance to security once data leaves GAS	100	4.27	1.07
Level of access to users	100	4.03	1.05
Exposure of confidential information	100	4.36	1.76
Vulnerability to cyber attacks	100	4.07	1.74
Disruption in operations system	100	2.74	1.54
Employees leaking confidential information	100	2.07	1.77
Protecting sensitive information	100	3.93	1.05
Loss of electronic files, USB keys and laptops	100	4.23	1.65
Cost of implementing information security	100	4.12	1.77
Ignorance of significance and the sensitivity of data	100	4.43	.78

Scale: 1=Very Low, 2=Low, 3=Moderate, 4=High, 5=Very High
(Source: Author's field study, 2013)

From Table 2, it can be seen that, compliance to security once data leaves GAS (mean=4.27), data security (mean=4.14), level of access to users(mean=4.03), exposure of confidential information (mean=4.36), vulnerability to cyber attacks (mean=4.07), loss of electronic files, USB keys and laptops (mean=4.27), cost of implementing information security (mean=4.12), protecting sensitive information (mean=3.98) and ignorance of significance and the sensitivity of data (mean=4.43) were rated as some of the challenges of IS at GAS. From the standard deviation, it can be seen that the dispersion is very small (ranging below 1.8) therefore the results can be depended upon. Employees leaking confidential information (mean=2.07), and disruption in operations system (mean=2.74) were rated as not being a challenge at GAS as asserted in the literature review supported by the interview responses.

It therefore suggests that GAS has many challenges regarding information security but serious information security problems with regard to leakage, and disruption of operating system were rated either low or very low

Section Logout

Table 3 answers the question "Is there any mechanism for session logout after a specified time?" This question was meant to assess the security measure on the machine in case a staff stopped using a computer. Again it is to check whether the IT policy was followed as seen in the secondary data.

Table 3: Section Logout

Section Logout	**Frequency**	**Percent**
Yes	88	88.0
No	12	12.0
Total	100	100.0

Source: Author's field study, 2013

Table 3 revealed that, 88.0% of the respondents reported that there were session logouts after a specified time while very few of them representing 12.0% reported that there were no session logouts. This means that, sessions logged out after a specified time as affirmed by majority of the respondents. This helps to protect the computer and data from external people.

Printing Document on Shared Printer

Figure 3 answers the question "do you print sensitive document like reports to the Auditor General on printers that other people may access?" This question was meant to determine if other people could have access to information that they were not supposed to have access to.

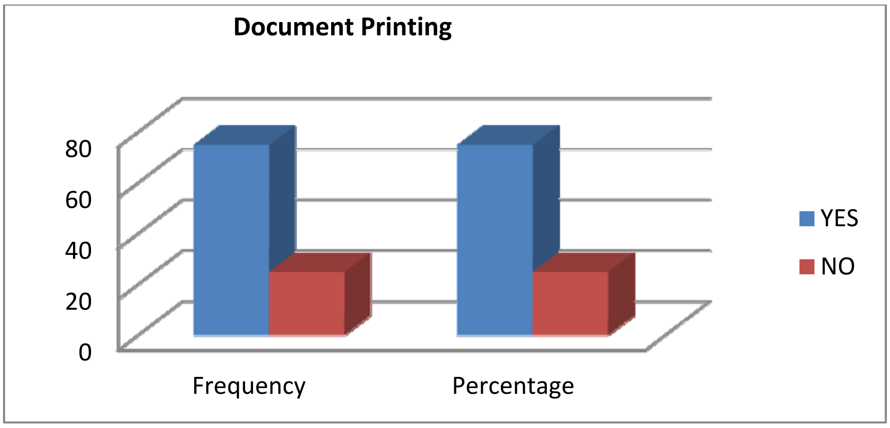

Figure 3: Printing Document on Shared Printer

Source: Author's field study, 2013

Figure 3 indicate that, 75% of the respondents said yes, with 25% saying no. This means that, sensitive documents were printed on shared printers. This is a threat to information since anybody who uses the printer may have access to any information that is printed. The printer could also be used to retrieve printed document. This was also confirmed from the interview and researchers' observation at GAS.

Padlock place of work when leaving workplace

Table 4 answers the question "Do you lock your office when you leave it, even if you are going for your lunch?" This question was meant to assess if information was safe as a measure to protect documents that were left open at the offices.

Table 4: padlock place of work when leaving workplace

Lock Office when Leaving Office	**Frequency**	**Percent**
Yes	63	63.0
No	37	37.0
Total	100	100.0

Source: Author's field study, 2013

Table 4 indicates that, 63.0% of the respondents said yes they locked their office when leaving for lunch while 37.0% said they did not lock their offices. This means that, majority of the respondents (about 3 out of 5) locked their office while some (about 2 out of 5) of them failed to lock them. This again means that, much of information was consciously kept out of reach of intruders. However in situations where computers were not logged off, intruders could still have access (37%) to information that was not consciously protected.

Reasons to Implement Information Security

Figure 4 answers the question "do you think it is necessary to implement information security at GAS?**"** This question was meant to determine whether it is necessary to implement IS looking at the cost in implementing it.

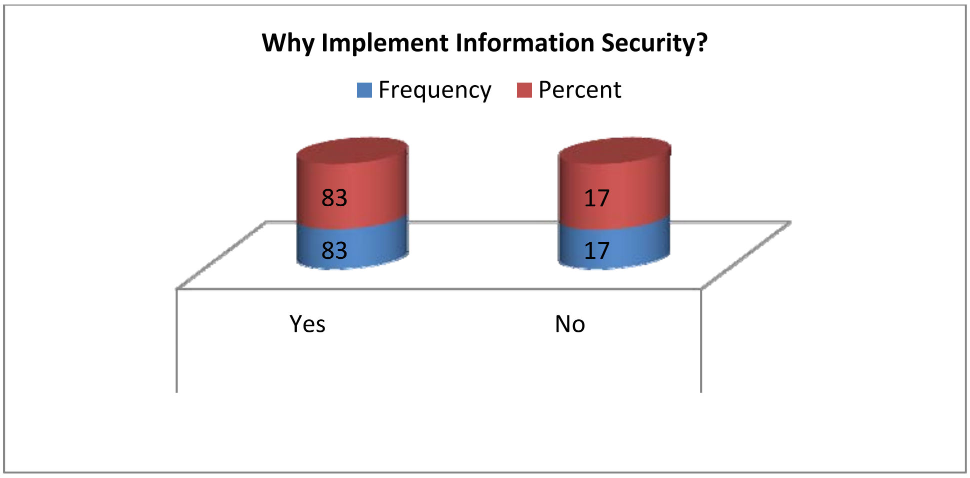

Figure 4: Reasons to Implement Information Security
Source: Author's field study, 2013

Figure 4 shows that, majority of the respondents (83%) said yes it is necessary to implement IS while few of them (17%)) said no it is not necessary. This means that majority of the respondents find Information Security to be a necessity at Ghana Audit Service.

Significance of Information Security at Ghana Audit Service

Table 5 answers the question "Which of the following will you agree as an importance of information security at Ghana Audit Service?" This question was meant to determine the importance of IS at GAS. The responses of the respondents were measured on a 5-point Likert type rating scale. The arithmetic mean and standard deviations were also calculated to confirm the effect of stress on performance. This was to compare with the responses from the interview with key staff

Table 5: Importance of Information Security at GAS

Importance of Information Security (IS)	N	Mean	Std. Deviation
Repercussions of information falling into the wrong hands can be embarrassing	100	4.07	.807
Lack of information security may lead to massive costs for GAS	100	4.33	1.35
Information security reduces frauds at GAS	100	4.36	1.76
Information security is the key to effective management of GAS	100	4.40	1.72
Information Security protect information against unauthorized acquisition	100	4.74	1.44
IS protects information against damage, disclosure, or manipulation	100	3.87	1.46
IS protects information against change and loss of information	100	3.93	1.17

Scale: 1=Very Low, 2=Low, 3=Moderate, 4=High, 5=Very High
Source: Author's field study, 2013

From table 5, it can be observed that respondents perceived that, the criteria used are indeed some of the key importance of IS at GAS. According to the result, repercussions of information falling into the wrong hands can be embarrassing (mean=4.07), lack of IS may lead to massive costs for GAS (mean=4.33), information security reduces frauds at GAS (mean=4.36), IS is the key to effective management of GAS (mean=4.40), IS protects information against unauthorized acquisition (mean=4.74), IS protects information against damage, disclosure, or manipulation (mean=3.87), and IS protects information against change and loss of information (mean=3.93) were rated high as some of the importance of IS at GAS. This means that, these reasons are some of the importance of IS at GAS which supports the findings in the literature reviewed. Key staffs were asked the same question. Their responses as outlined in the interview responses agreed with this response from the staff. According to the IT officer, the impact of information security is enormous as elaborated in the interview analysis.

Additional Importance of Implementing IS at GAS

The respondents were asked "what do you think is the reason for implementing Information security despite its cost?" Using the interview data gathering instrument, this question was meant to explore the other importance of IS that were not captured in the questionnaire. The respondents listed the following as some of the important reasons of implementing Information Security at GAS:

- To protect information from damage.
- To enhance professionalism, image, integrity and confidentiality of GAS information
- To safeguard information, prevent unauthorised access and reduce risk
- To enhance efficiency and reliability of information
- It helps to reduce legal issues from clients. This is because, audited organizations who see their records in the public domain, may resort to court action.
- It increases confidence and trust by clients. Clients will not be afraid of any piece of information given to the audit service, because they are assured of anonymity and information security and protection from other third parties.

Summary of the Findings

Challenges of Information Security (IS)

The study indicated that, there are potential challenges to IS at GAS. The study revealed the following as some of the challenges of IS at GAS:

- Inadequate education on information security at GAS. Many of the personnel lack adequate knowledge in information security processes such as scanning and encrypting data.
- Antivirus is not updated as frequent as expected.
- Documents are not adequately protected.
- There is a seeming lack of compliance to security issues, standards and policy on information security.
- Data security seems not to be a paramount issue.
- The likelihood of unathorised people having access to information is high.
- Exposure of confidential information needs to be mitigated or eliminated
- Vulnerability to cyber attacks
- Loss of electronic files, USB keys and laptops.
- Cost of implementing information security.
- Suspected ignorance of significance and the sensitivity of data
- Pressure from colleagues to share security password with them.
- The use of one computer system by different users.
- Staffs using their personal laptops to process and store official information
- Low users' involvement in implementing security. Some users forget their passwords, complain about many passwords and secure locking of offices when going out not the best.
- Use of Auditors' pen drives on their clients' computer could leak vital audit information to the clients.
- When GAS computers are auctioned, the hard drives are mostly not removed, which could leak vital information.
- The threat posed by authorized users sometimes giving their user-names and passwords to unauthorized users.
- Occasionally some of GAS information is inadvertently not updated into the database. This leads to the difficulty in tracing some important documents.
- Finally, GAS sensitive information is sometimes inadvertently left open at the registry. This means that, any aunathorised person entering the registry could have unathorised access to such information.

Importance of Information to GAS

It came out that, majority (83%) of the respondents find IS as a necessity at GAS. From the study, it came out that IS has the following importance:

- It helps to trace users who may alter or misuse information at GAS.
- It helps to prevent or reduce information fraud in the service.
- It enhances confidentiality and integrity of information at GAS.
- IS protects assets of GAS from third parties.

- It eliminates embarrassing repercussions of information falling into the wrong hands.
- Lack of IS may lead to massive costs for GAS.
- IS the key to effective, efficient and reliable management of GAS information
- IS protects information against unauthorized access, and reduces risk and disclosure.
- IS safeguards GAS information against change, manipulation, or loss.
- IS protects information from damage.
- IS enhances professionalism, image, integrity and confidentiality of GAS information.
- It helps to reduce legal issues from clients.
- It increases confidence and trust by clients.

Encryption of Transferred Data: The study revealed that, transmission of information to different stakeholders and department are normally encrypted. The type of encryption used is "Read Only" thus, users are not able to alter the content in the data. It also came out that, only information on Compact Disk (CD) is encrypted but those transmitted through E-mails such as notes and reports are not encrypted.

Sensitivity of Stored Information: It came out that, sensitive information is stored on the server. Backups on one external drive and one laptop off site are kept for the whole region. The study indicates that, weekly updates are executed and backups are also tested weekly to make sure sensitive information is not lost in case of disaster.

Standards to Ensure Information Security: The study revealed that, there are standards at GAS but these standards are not properly followed. Users also complain about the standards. It also came out that, there are CCTV cameras in Accra server room but GAS Kumasi is now trying to implement such security measure to protect information. Measures are in place to use users' biometric data to give access into server room and the server.

Making Sure Information is Secured: The researchers came out with the following as ways of securing information at GAS:

- Staffs are to be advised to treat all information as confidential.
- Periodic education ought to be given to the staff on the implication of not securing information at GAS.
- Users could be prompted monthly to change their passwords. If they fail to change them, the computer could be programmed to be locked-up automatically.

How User Accounts are managed: The study revealed that, users accounts are created by only the IT Administrators, and users are not allowed to re-activate their accounts when they are blocked. When wrong passwords are entered for three consecutive times, the account is blocked automatically. It also came out that, users are verified by the IT Administrator before issuing any password.

How Information is transferred: The study indicates that, information is transferred to other district/units by hard copies of document, through E-mail, telephone and pen drives.

Section Logout: The study revealed that, login sessions logout after a specified time as 92% of the respondents affirmed it. Majority of the respondents lock their offices. Sensitive documents are printed on shared printers.

Conclusion

The aim of the study was to evaluate information security in public organizations such as the Audit Service in terms of the information security policies practiced, the problems as well as challenges of securing information. The study revealed that the Audit Service like most public organizations does not effectively manage its information as most employees of the case institution have inadequate basic knowledge in information systems, and information security. The Audit Service, again like most public organizations, encounters numerous challenges, making it difficult for the agency to effectively manage its data (information systems). Managers of organizations such as the Audit Service have to seriously invest in their human resources so as to equip their personnel to protect sensitive information that may be potentially harmful if accessed or leaked.

References

[1] Åhlfeldt, R. (2001). *Information security in home healthcare personal integrity and secrecy*. Ph.D thesis, Skövde, SWEDEN, 2001.

[2] Abrar ul Haq on current issues (March 4, 2013): News 7/11

[3] Barnard, L. & von Solms, R. (2000). A formalized approach to the effective selection and evaluation of information security controls. *Computers and Security*.19 (2), pp.185-194.

[4] Frost, & Sullivan. (2011). *The global information security workforce study*. A Frost & Sullivan Market Survey CISSP Global Program Director, Information Security.

[5] Iran Audit Organization. (2007). *A Preface to Accounting Standards*. Retrieved from http://audit.org.ir/media/standards/86.pdf.

[6] Kearns, P. (n.d), The public sector needs to wake up to the importance of protecting its confidential information from being lost or stolen. Shred-it. Available at URL: http://ebookbrowse.com/gdoc.php?id=272711241&url=6ee49256a1c4cdecb7c10b04d649fcf0 [Accessed on 12/05/2012]

[7] Lehtinen, R., Russel, D. & Gangemi, G. (2006). *Computer security basics*. Sebastopol, CA: O'Reilly Media, Inc.

[8] Mahmood, K., & Ashrafullah. (2010). *Information security management of healthcare system - a case study of blekinge region healthcare*. Master Thesis, Computer Science

[9] Nosworthy, J. (2000). Implementing information security in the 21st century - Do you have the balancing factor? *Computers and Security* 19(4): 337-347.

[10] Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. (5th ed.).

[11] Edinburg Gate, England: Pearson Education Limited.

[12] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). An analysis of end user security behavior, computer & security, 24, 124-133

[13] Zohreh, D. S., Jamshid, S. S., & Vahid, N. F. (2004. *The interaction model of business strategy with research and development strategy and effect of this interaction on organizational performance in iran's pharmacy industry*. Tehran, Iran.