RELATIONSHIP BETWEEN INDUSTRY BEST PRACTICES AND INFORMATION SECURITY BREACH INCIDENTS OF SACCOS IN KENYA

Jerotich Sirma, George Raburu

School of Informatics and Innovative Systems

Jaramogi Oginga Odinga University of Science and Technology

P.O. Box 210-40601, BONDO-Kenya

N. B. Okelo

School of Mathematics and Actuarial Science

Jaramogi Oginga Odinga University Science and Technology

P.O. Box 210-40601, BONDO-Kenya

ABSTRACT

Information is an important organizational asset that that is mainly vulnerable to attacks from user error, hackers and crackers, viruses and cyber criminals. This has resulted in loss of trillions of dollars around the world and over 4 billion shillings in East Africa. The study investigated whether information security policies assist in preventing unauthorized individuals from accessing SACCOS' sensitive information. The study looked at the relationship between dependent and independent variables. The study investigated the relationship between industry best practices and information security breach incidents The study used correlational survey as its research design. The study utilized a questionnaire as a survey instrument to collect responses from 85 SACCOS IT personnel with regard to their perceptions of how information security policies affect computer security breach incidents. Coefficient of variation was used to determine the sample size of 85 SACCOS registered with SASRA. Further, Simple random sampling was used to select 85 SACCOS. From the 85 SACCOS, one IT personnel was selected using simple random sampling from each SACCOS to obtain 85 IT personnel from a total of 270 IT personnel from 135 SACCOS registered with SASRA. A pilot test was carried out to test the validity of the survey instrument. Cronbach's alpha coefficient was used to assess the internal reliability of the research instrument. Quantitative data was analyzed by using Statistical Package for Social Sciences (SPSS) version 22. Research hypotheses were tested using both 2 tailed t-tests and analysis of variance (ANOVA) tests. Pearson correlation was conducted to test the relationship between independent variables and dependent variable. Regression analysis was used to show the contribution of each independent variable to the dependent variable. Null hypothesis was tested at 95% level of confidence. If the p-value obtained is less than 0.05, then the null hypothesis was rejected, but if the p-value obtained was more than 0.05, then the null hypothesis was accepted. The results of the study revealed that there is a weak relationship between information security policies and security breach incidences in the SACCOS sector

INTRODUCTION

Information is an important organizational asset that is subject to vulnerability to attacks due user error, hackers and crackers, viruses and cyber criminals. With the increase of cyber users in the world, cyber crimes and threats has increased in Africa as evident by the study of Kritzinger & Solms (2012). The Savings and Credit Cooperative Societies (SACCOS) sector must prioritize the security of computer systems to safeguard the accuracy, confidentiality and availability of their information assets to its users (Doherty & Fulford, 2005). SACCOS are entrusted with highly confidential and privileged client financial information. Subsequently, SACCOS have an obligation to maintain, store, and secure this sensitive information and to ensure their clients' privacy (Comerford, 2006). The underlying problem in most organizations is managing information security policies. Information security entails the creation of policy statements used in ranking information risks, identifying acceptable security goals and procedures of a SACCOS (Da Veiga & Eloff, 2007; Laudon & Laudon, 2012; Metzler, 2007; Robinson, 2005). Studies have identified good security policies (Kritzinger & Solms, 2012; Dhillon and Torkzadeh 2006) and frameworks for security governance (Brotby 2009; Da Veiga and Eloff 2007; Ula, Ismail & Sidek, 2011.; Vonn Solms & Von Solms 2009), yet there is still lack of understanding by users about how security breach incidents have the potential to weaken the implementation of security policies in the SACCOS sector. Security breaches are incidents consisting of unauthorized access to sensitive or confidential data (Kraemer & Carayan, 2007) of a SACCOS. Security breaches can also arise through computer programs that replicate viruses across systems and networks; intrusion of organizational computer systems by unauthorized outsiders who can manipulate data; abuse of systems that contain data; theft of valuable hardware, software and information assets; financial systems are vulnerable to individuals with the intention to defraud an organization; destruction or incorrect entry of data by computer users; disasters such as earthquakes, floods or fires can destroy computing facilities or data resources; and computer systems can be damaged by angry employees who is seeking revenge from an organization (Doherty & Fulford, 2005; Laudon & Laudon, 2012).

Information security policies are designed to safeguard network resources from security breaches (Doherty & Fulford, 2005). Information security polices outline the responsibilities and acceptable user actions of SACCOS employees when using SACCOS computers and networks. Security controls include management controls, operational controls, and technical controls. Information security policies are considered to be the management control measures that will define an appropriate security for the network infrastructure (Alshboul, 2010; Post & Kagan, 2007). Other management controls include vulnerability assessment and security plans implemented to manage the security (Salmela, 2008) of the SACCOS. Security policies have clear rules on how a network can be accessed while maintaining confidentiality and identifying the ramifications of a security breach (Greene, 2006; Whitman & Mattord, 2008) of the SACCOS. Operational controls include physical security, personal security, business continuity planning, incident response, hardware and software maintenance, confidential data protection, and security awareness training (Albrechtsen, & Hovden, 2008; Bowen, Hash & Wilson, 2006; Hagen, 2008, Richardson, 2011) that are implemented by SACCOS personnel as opposed to computer software automation process.

RESULTS AND DISCUSSION

Adoption of industry best practices is set forth on tables 12, 13 and 14. Table 12 presents the results of how often SACCOS audit and enforce the documented IT security policy. 55.6 percent (40) audits and enforces every year, 29.2 percent (21) audit and enforces in less than 1 year, 11.1 percent (8) in every two years, 1.4 percent (1) has never audited and enforced the documented IT security policy, while 2.8 percent (2) did not know if they perform audit and enforce documented IT security policy.

Table 1: Auditing and enforcing documented IT Security Policy

Audit and Enforce IT Policy	Frequency	Percentage	Cumulative Percentage
Never	1	1.4	1.4
Every 2 years	8	11.1	12.5
Do not know	2	2.8	15.3
Every year	40	55.6	70.9
Less than 1 year	21	29.2	100

Source: Research Data (2015)

Table 13 presents the results of how often IT security policies audited by an independent third party. 54.2 percent (39) audits every year, 23.6 percent (17) audits every two years, 12.5 percent (9) do not audit, 6.9 percent (5) do not know, and 2.8 percent (2) audits in less than one year.

Table 2: Auditing of IT Security by an Independent Third Party

IT Security Policies Audited	Frequency	Percentage	Cumulative Percentage
Never	9	12.5	12.5
Every 2 years	17	23.6	36.1
Do not know	5	6.9	43
Every year	39	54.2	97.2
Less than 1 year	2	2.8	100

Source: Research Data (2015)

Table 14 presents the responses and percentages for the importance of best practices success factor on IT security implementation in SACCOS. In ensuring security policy reflects business objectives, 58.3 percent (42) of the respondents found it very important to the operations of their SACCOS. 48.6% (35) of the respondents deemed very important for their SACCOS to implement security that is consistent with their culture. Respondents also reported that 47.2 percent (34) found it very important and extremely important to have commitment from management regarding adoption of industry best practices. 69.4 percent (38) of the respondents indicated the extreme importance of a good understanding of security requirements by SACCOS employees. Effective marketing of security to all SACCOS employees or other members of the SACCOS had the highest score of 48.6 percent (35) in terms of importance. 44.4 percent (32) of the respondents reported that it was very important to distribute guidelines on IT security policy to all SACCOS' employees or other members of SACCOS. Over half of the respondents (56.9 percent) found extremely important to provide appropriate training and education to all SACCOS' employees and other members. Comprehensive measurement system for evaluating performance in security management had 50 percent (36) of the respondents reporting the factor as very important. 43.1 percent (31) of the respondents deemed very important in provision of feedback system for and education to all employees or other members of SACCOS.

Table 3: Importance of best Practices Success factors on IT security

Factors	Not Applicable	Not important	Somewhat important	Very Important	Extremely Important
Ensuring security policy reflects business objectives	0% 0	0% 0	2.8% 2	58.3% 42	38.9% 28
An approach to implementing security that is consistent with the SACCOS culture	1.4% 0	5.6% 4	16.7% 12	48.6% 35	27.8% 20
Visible commitment from Management	1.4% 1	0% 0	4.2% 3	47.2% 34	47.2% 34
A good understanding of security risks	0% 0	0% 0	1.4% 1	29.2% 21	69.4% 50
A good understanding of security requirements	0% 0	0% 0	4.2% 3	43.1% 31	52.8% 38
Effective marketing of security to all SACCOS employees or other members of the SACCOS	5.6% 4	0% 0	18.1% 13	48.6% 35	27.8% 20
Distribution of guidance on IT security policy to all SACCOS employees or other members of the SACCOS	1.4% 1	1.4% 1	19.4% 14	44.4% 32	33.3% 24
Providing appropriate training and education to all employees or other members of the SACCOS	1.4% 1	0% 0	5.6% 4	36.1% 26	56.9% 41
Comprehensive measurement system for evaluating performance in security management	1.4% 1	4.2% 3	6.9% 5	50% 36	37.5% 27
Provision of feedback system for and education to all employees or other members of the SACCOS	1.4% 1	4.2% 3	19.4% 14	43.1% 31	31.9% 23

Source: Research Data (2015)

4.7 Scope of Information Security Policy

Table 15 presents the responses and percentages for each security issues covered in IT security policies and/or supplementary procedures or standards in respondent's SACCOS. Encryption and Mobile computing had the highest percentage of 59.7 in policy document only category. Personal usage of Information Systems followed with 50 percent, Internet access had

47.2 percent, disclosure of information had 45.8 percent, Viruses, worms & Trojans had 43.1 percent, Contingency planning had 41.7 percent, Software development and physical security had the same percentage of 36.1, violations and breaches had 34.7 percent and system access control had 25 percent. On the category of policy document and supplementary procedure or standard , System access control had the highest 75 percent, violations and breaches had 65.3 percent, Software development and physical security had the same percentage of 63.9, contingency planning had 58.3 percent, viruses, worms & Trojans had 56.9 percent, disclosure of information had 54.2 percent, Internet access had 51.4 percent, personal usage of information systems had 50 percent, and encryption and mobile computing had the lowest percentage of 40.3

Table 4: Relationship between industry best practices and information security breach incidents

Correlations			
		Security breach incidences	Industry best practices
Security breach incidences	Pearson Correlation	1	-.026
	Sig. (2-tailed)		.831
	N	72	72
Industry best practices	Pearson Correlation	-.026	1
	Sig. (2-tailed)	.831	
	N	72	72

Source: Research Data (2015)

Table 20 presents the results of the relationship between information security breach incidences of SACCOS with an information security policy with a broad scope and information security breach incidences of SACCOS without and the correlation is significant because the r value is 0.500 and the p-value is 0.000 which is <0.05. Therefore the null hypothesis is rejected. The results indicate that SACCOS with broad scope are in a better position in addressing their security breach incidents and severity than SACCOS without a broad scope.

CONCLUSION

. The results demonstrated no evidence of a statistically significant relationship between the adoption of industry best practices and reported security breach incidents. These results are consistent with Doherty and Fulford (2005) findings of no significance. However, further research is required to determine whether the increased perception and reporting of security breaches by SACCOS that have incorporated industry best practices into their respective information security departments may correlate with the level of sophistication within SACCOS' information security IT departments. In ensuring security policy reflects business objectives, 58.3 percent (42) of the respondents found it very important to the operations of their SACCOS. 48.6 percent (35) of the respondents deemed very important for their SACCOS to implement security that is consistent with their culture. Respondents also reported that 47.2 percent (34) found it very important and extremely important to have commitment from management regarding adoption of industry best practices. 69.4 percent (38) of the respondents indicated the extreme importance of a good understanding of security requirements by SACCOS employees. Effective marketing of security to all SACCOS employees or other members of the SACCOS had the highest score of 48.6 percent (35) in terms of importance. 44.4 percent (32) of the respondents reported that it was very important to distribute guidelines on IT security policy to all SACCOS' employees or other members of SACCOS. Over half of the respondents (56.9 percent) found extremely important to provide appropriate training and education to all SACCOS' employees and other members. Comprehensive measurement system for evaluating performance in security management had 50 percent (36) of the respondents reporting the factor as very important. 43.1 percent (31) of the respondents deemed very important in provision of feedback system for and education to all employees or other members of SACCOS.

Over one-half of SACCOS' respondents (50%) reported use of Policy document and supplementary procedure or Standard for disclosure of information. system access control. Internet access, viruses, worms & Trojans, software development, contingency planning, personal usage of Information Systems, physical security, violations and breaches. On encryption and mobile computing, respondents reported a tie of 40.3 percent while using policy document and supplementary procedure or Standard regarding IT security issue. Security issues covered in IT security policy document only had encryption and mobile computing reporting more than 50 percent were in place, personal use of information systems reported 50 percent, while close to half of the respondents' reported system access control at 25 percent, software development at 36.1 percent, physical security at 36.1 percent, and violations and breaches at 34.7 percent

REFERENCES

Adebayo, A., Omotosho, O., and Adekunle, Y. (2012). Statistical Insight into Breach Data toward improved Countermeasures. *Information and Knowledge Management* 2(8):17-23.

Akuta, E., Ong'oa, I., and Jones, C. (2011). Combating Cyber Crime in Sub-Sahara Africa; A on Law, Policy and Practice,' *Journal of Peace, Gender and Development* 1(4):129-137.

Baker, W. H. and Wallace, L. (2007). Is information security under control? Investigating quality in information security management. *IEEE Security & Privacy*, 5(1):36-44.

Basta, A. and Halton, W. (2008). Computer Security and Penetration Testing, Boston, M.A: Thomason Course Technology.

Berg, G. G., Freeman, M. S. and Schneider, K. N. (2008). Analyzing the TJ Maxx data security fiasco: Lessons for auditors. *The CPA Journal*, *78*(8):34-37.

Creswell, J. (2009). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (3rd edition), Thousand Oaks, CA: Sage Publications, Inc.

Curtin, C. M., and Ayers, L. T. (2009). Using science to combat data loss: Analyzing breaches by type and industry. *I/S: A Journal of Law and Policy for the Information Society*, 4(3):569-601.

D’arcy, J., and Hovav, A. (2009). Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics: Supplement*, 89:59-71.

Da Veiga, and Eloff, J. H. P. (2007). “An Information Security Governance Framework.” *Information Systems Management* 24(4):361-372.

Desouza, K. C. (2008). The neglected dimension in strategic sourcing: security. *Strategic Outsourcing: an International Journal*, 1(3):288-292.

Dhillon, G. (1997). Managing Information System Security. London, MacMillan

Doherty, N. F., and Fulford, H. (2006). Aligning the information security policy with strategic information systems plan. *Computer & Security*, 25:55-63.

Farn, K-J., Lin, S-K., and Lo, C-C. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interface*, 30(1):1-7.

Fordham, D. R. (2008). How strong are your passwords? *Strategic Finance*, 89(11):42-47.

Fraenkel, J. R and Wallen, N. E. (2000). How to design and evaluate research in education, (4th edition), Mc GrawHill Publishers, Boston

Greene, S.S., (2006). Security Policies and Procedures: Principles and Practices, Upper Saddle River, NJ: Pearson Education, Inc.

Greene, S. (2014). Security Program and Policies: Principles and Practices (2nd edition), Upper Saddle River, NJ: Pearson IT Certification

Greenleaf, G (2012). Global data privacy laws: 89 countries, and accelerating. *Privacy Laws &Business International Report, Issue 115. Queen Mary School of Law Legal Stud Research Paper No. 98/2012* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000034

Gorga, E., and Halberstam, M. (2007). Knowledge inputs, Legal institutions and firm structure: Towards a knowledge-based theory of the firm. *Northwestern University Law Review*; 10(3):1123-1206.

Gunasekara, G. (2007). The 'final' privacy frontier? Regulating trans-border data flows. *International Journal of Law and Information Technology, 15*(3):362.393.

Gupta and Sherman (2012) Determinants of Data Breaches: A Categorization-Based Empirical Investigation, *Journal of Applied Security Research*, 7(3):375-395.

Hagen, J. M., Albrechten, E. and Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4):377-397.

Harrison, W. (2006). Passwords and passion. *IEEE Software*, 23(4):5-7.

Heikkila, F. M. (2007). Encryption: Security considerations for portable media devices. *IEEE Security & Privacy*, 5(4):22-27.

Hong, K-S., Chi, Y-P, Chao, L. R., and Tang, J-H. (2006). An empirical study of information security policy on information security elevation in Taiwan. *Information Management & Computer Security, 14*(2):104-115.

Holloway, M. and Fensholt, E. (2009). HITECH: HIPAA gets a facelift. *Benefits Law Journal, 22*(3):85-89.

Hook, B. (2009). Reducing risk. *SC Magazine*, 20(5):26-28

Humphreys, E. (2007). *Implementing the ISO/IEC 27001: Information Security Management System* Standard, Boston, M.A: Artech House

Information security breaches survey (2013) Retrieved from http://www.nlondon.bcs.org/pres/cpapr13.pdf

Johnson, A. C. and Warkentin, M. (2008). Information privacy compliance in the healthcare industry. *Information Management & Computer Security*, 16(1):5-19.

Keller, S., Powell, A., Horstmann, B., Predmore, C., and Crawford, M. (2005). Information security threats and practices in small businesses. *Information Security Management*, 22(2):7-19.

Kent, K. and Souppaya, M. (2006). Guide to computer security log management. NIST Special Publication 800-92. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf

Khalifa, N.H. (2013). Information Technology Capabilities in Enabling Electronic Banking: Case Study of a Bank in a Developing Country. *Journal of Electronic Banking Systems*, 2013:1-28

Kothari, C.R., (2012), Research Methodology: Methods and Techniques, (2nd edition), New AGE International Publishers, New Delhi, India

Kumar, R. L., Park, S. and Subramaniam, C. (2008). Understanding the value of countermeasures portfolios in information systems security. *Journal on Management Information Systems*, 25:243-279.

Nahra, K. J. (2008). HIPAA security enforcement is here. *IEEE Security & Privacy,* 6(6):70-72.

Nassiuma D.K. (2000) Survey Sampling: Theory and Methods. University of Nairobi Press, Nairobi.

Nation Newspapers. (2012, December). Bank reassures customers after spate of ATM card fraud in city. Retrieved from Nation Newspaper Website http://www.nation.co.ke/business/news/Bank-reassures-customers-after-spate-of-ATM-card- fraud-in-city--/-/1006/1651892/-/yrpfk4z/index.html

Nation Newspapers. (2014, July). Banks lose Sh60m in electronic theft Retrieved from Nation Newspaper Website http://www.nation.co.ke/news/Banks-lose-Sh60m-in-electronic-theft/1056/2382722/ck0wga/-/index.html

Nyanchama, M. (2005). Enterprise vulnerability management and its role in information security management. Information Systems Security, 14:9-56.

Oso ,W.Y and Onen, D. (2009). Writing Research Proposal and Report. Nairobi: Sitima

Otto, P. N., Antón, A. I., and Baumer, D. L. (2007). The ChoicePoint dilemma: How data brokers should handle the privacy of personal information. *IEEE Security &*

Privacy,*5*(5):15-23.

Poepjes, R., and Lane, M. (2012) An Information Security Awareness capability Model (ISACM) *Australian Information Security Management Conference Proceedings of the 10th Australian Information Security Management Conference*, Perth, Western Australia, December 3-5:1-8.

Richardson, R. (2011). 2010/2011 CSI computer crime and security survey. *GOCSI.com*. Retrieved from https://cours.etsmtl.ca/gti619/documents/divers/CSIsurvey2010.pdf

Robinson, T. (2005). Data security in the age of compliance. *networker*, 9(3):24-30.

Rouse, M. (2010). Data Breach. Retrieved from http://searchsecurity.techtarget.com/definition/data-breach

Romanosky, S., Telang, R., and Acquisti, A. (2008). Do data breach disclosure laws reduce identity theft? *Seventh Workshop on the Economics of Information Security*, Hanover, NH, 25(28):1-20.

Rotvold, G. (2008). How to create a security culture in your organization. *Information Management Journal*, 42(6):32-34.

Salmela, H. (2008). Analysing business losses caused by information systems risk: A business process analysis approach. *Journal of Information Technology*, 23(3):185-202.

Schwartz, P. M. and Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105(5):913-984.

Sekaran, U. (2003). Research methods for business (4th edition), Hoboken, NJ: John Wiley & Sons.

Shostack, A and Stewart, A. (2009). The new approach to Information Security. Harlow, Essex Pearson Education Ltd.

Siponen, M. T., and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. The Database for Advances in Information Systems, 38(1):60-80.

Stream, G., and Fletcher, J. (2008). Demystifying computer networks for small practices. *Family Practice Management*, 15(1):25-28.

SolarWinds, (2013)**.** Key Considerations in Protecting Sensitive Data Leakage Using Data Loss

Prevention Tools. Retrieved from http://web.swcdn.net/creative/pdf/Whitepapers/Key_Considerations_for_Effective_Data_Loss_Prevention.pdf.

The Data Protection Bill 2013 retrieved from https://www.google.com/?gws_rd=ssl#q=data+protection+bill+2013+kenya

Ula, M., Ismail, Z. B., and Sidek, Z. M. (2011). A Framework for the Governance of Information Security in Banking System, *Journal of Information Assurance & Cybersecurity*, 2011:1-12.

U. S. Department of Commerce. (2014). Safe Harbor certification. Export.gov. Retrieved from http://www.export.gov/safeharbor/.

Verdon, D. (2006). Security Policies and the software developer. *IEEE Security & Privacy*, 4(4): 42-49.

Weaver, R. (2007). Guide to Network Defense and Countermeasures Second Edition. Boston, MA: Thomson Course Technology.

Whitman, M. E. and Mattord, H. J. (2008). Management of Information Security (2nd edition) Boston, MA: Thomson Course Technology.