SECURITY BREACH INCIDENCES OF SACCOS WITH OR WITHOUT SECURITY POLICY WITH A BROAD SCOPE: A CASE 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

The risks that organizations face include safeguarding information resources in their networks. Organizations have formulated security policies with the hope of solving the problem of security breaches or to significantly reduce incidences of security breaches. However, systems are still vulnerable to security breaches. The vulnerability may arise from security breaches that could be internal or external to the organization. A security breach can result in the risk of an intrusion into the SACCOS' sensitive information. For example, an intruder can potentially gain access to SACCOS client documents that may contain propriety financial information. Disclosure of client information can result in the loss of confidence in SACCOS and real financial loss. Despite the identification of good security policies and frameworks for security governance in the information systems field, 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. The study will try to fill in the gap upon reporting the results of the study that sought to analyze the relationship between information security policies and the incidences of security breaches in the SACCOS sector in Kenya.

INTRODUCTION

This study analyzed the impact of information security policies in Kenyan SACCOS. Subsequently, the study examined information security policies and computer security breach incidents in relation to protecting customer data. The study also reviewed topics relevant to security and data breach incidents, data threats, and information security assessment procedures.

1.7 Scope of the Study

The study was confined to an impact of information security policies on security breach incidences in Kenyan SACCOS. The study targeted 170 IT personnel from 85 selected SACCOS in Kenya that are registered with SASRA that formed the population of the study

1.8 Limitation of the Study

The findings of the study were limited to 85 selected SACCOS with a population of 170 IT personnel in Kenya who are registered with SASRA. The study will be limited to the information provided by the respondents. However, the delimitation of this study was the lack of exhaustive survey of all 135 SACCOS registered with SASRA which was beyond the scope of this study. However, an overview of 85 selected SACCOS was discussed in this study.

1.10 Assumptions of the Study

The study was undertaken under the following assumptions:

i. Most SACCOS Information Technology (IT) personnel have access to information security policies of the SACCOS
ii. Respondents for the study will make effort in completing the assigned questionnaire on time and answer all the questions fully and truthfully
iii. The collected responses will be a representative of the current situation of information security breach incidences and severity in the SACCOS sector
iv. The term “members” will exclude online SACCOS clients

RESULTS AND DISCUSSION

Table 1: Security issues covered in IT security policy document and/or through supplementary procedures or standards

IT Security Issue	Policy Document Only	Policy Document and Supplementary Procedure or Standard
Disclosure of Information	45.8% 33	54.2% 39
System access control	25% 18	75% 54
Internet access	47.2% 34	51.4% 37
Viruses, worms & Trojans	43.1% 31	56.9% 41
Software development	36.1% 26	63.9% 46
Contingency planning	41.7% 30	58.3% 42
Encryption	59.7% 43	40.3% 28
Mobile computing	59.7% 43	40.3% 29
Personal usage of Information Systems	50% 36	50% 36
Physical security	36.1% 26	63.9% 46
Violations and breaches	34.7% 25	65.3% 47

Source: Research Data (2015)

4.8 Uses of risk assessments, network vulnerability scans/penetration tests

Table 16 present a security measure of SACCOS employees when under a time deadline to finish an assignment using a five-point Likert scale (1=not at all likely to 5=Extremely likely)

The respondents were asked the likelihood of by-passing information security measures in order to complete a task. The results indicated that majority of the SACCOS are not very likely to by-pass a security measure when under deadline to complete a task. Under not very likely category, Scan a file for viruses reported 36.1 percent (26), install security software updated had 26.4 percent (19), install a digital certificate 33.3 percent (24), and install an ActiveX control form an unknown source had 41.7 percent (30). Under very likely category, Scan a file for viruses reported 33.3 percent (24), install security software updated had 34.7 percent (25), install a digital certificate 27.8 percent (20), and install an ActiveX control form an unknown source had 20.8 percent (15). Under Extremely likely category, Scan a file for viruses reported 19.4 percent (14), install security software updated had 26.4 percent (19), install a digital certificate 11.1 percent (8), and install an ActiveX control form an unknown source had 8.3 percent (6). Under not at all likely category, Scan a file for viruses reported 9.7 percent (7), install security software updated had 11.1 percent (8), install a digital certificate 19.4 percent (14), and install an ActiveX control form an unknown source had 25 percent (18). Overall results indicate that most of the employees knew about the use of security measure in place when under a deadline to complete an assignment within the SACCOS.

Table 2: SACCOS employees under deadline to finish an assignment

Statement	**Not at all Likely**	**Not very likely**	**Do not know**	**Very likely**	**Extremely likely**
Scan a file for viruses	9.7% 7	36.1% 26	1.4% 1	33.3% 24	19.4% 14
Install security software Updates	11.1% 8	26.4% 19	1.4% 1	34.7% 25	26.4% 19
Install a digital certificate	19.4% 14	33.3% 24	8.3% 6	27.8% 20	11.1% 8
Install an ActiveX control from an unknown source	25% 18	41.7% 30	4.2% 3	20.8% 15	8.3% 6

Source: Research Data (2015)

Table 3: Performance of security tasks

Statement	Not at all	Once a Year	Do not know	Once a Month	Every Day
Perform a vulnerability assessment that scanned the SACCOS networks to identify potential security risks.	8.3% 6	27.8% 20	4.2% 3	26.4% 19	33.3% 24
Hire an outside consultant to perform a risk assessment to identify the potential threats, probabilities, and impact of threats to the SACCOS' management controls, operational controls, and technical controls.	25% 18	59.7% 43	9.7% 7	5.6% 4	0% 0
Conduct an in-house risk assessment of security threats performed by the members of the SACCOS IT department and/or information security department.	6.9% 5	52.8% 38	4.2% 3	30.6% 22	5.6% 4
Provide employee training sessions on information security awareness and incident reporting	16.7% 12	62.5% 45	2.8% 2	15.3% 11	2.8% 2
Use managed security services of a third party	50% 36	22.2% 16	9.7% 7	1.4% 1	16.7% 12
Encrypt e-mail messages	50% 36	5.6% 4	5.6% 4	4.2% 3	34.7% 25
Review the information Security policies of the SACCOS	8.3% 6	84.7% 61	1.4% 1	2.8% 2	2.8% 2
Revise the information security policies of the SACCOS	9.7% 7	84.7% 61	2.8% 2	0% 0	2.8% 2

Source: Research Data (2015)

Table 17 presents the percentages and frequency of security tasks in the past 12 months based on respondents of the SACCOS under the study Over 50 percent of the respondents indicated that once a year they hire an outside consultant to perform a risk assessment to identify the potential threats, probabilities, and impact of threats to the SACCOS' management controls, operational controls, and technical controls, conduct an in-house risk assessment of security threats performed by the members of the SACCOS IT department and/or information security department, provide employee training sessions on information security awareness and incident reporting, review the information security policies of the SACCOS, and revise the information security policies of the SACCOS. 50 percent of the respondents reported that they do not use managed security services of a third party or encrypt e-mail messages. Performance of security tasks on a daily basis indicated that 33.3 percent (24) of the respondents performed a vulnerability assessment that scanned the SACCOS networks to identify potential security risks and 34.7 percent (25) reported that they encrypt e-mail messages.

Table 4: 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

Correlations				
		Security breach incidences	Narrow scope	Broad scope
Security breach incidences	Pearson Correlation	1	.015	.500**
	Sig. (2-tailed)		.900	.000
	N	72	72	72
Narrow scope	Pearson Correlation	.015	1	-.859**
	Sig. (2-tailed)	.900		.000
	N	72	72	72
Broad scope	Pearson Correlation	.500**	-.859**	1

	Sig. (2-tailed)	.000	.000	
	N	72	72	72
**. Correlation is significant at the 0.01 level (2-tailed).				

Source: Research Data (2015)

Table 21 presents the relationship between the uses of risk assessments, network vulnerability scans, and/or penetration tests and security breach incidents and results present r value of 0.052 and a p-value of 0.663 indicating there is no statistical significance between the variables. The study as a result accepts the null hypothesis. This means that SACCOS need to be more proactive in safeguarding their information by employing security techniques in their organization so that they can reduce security breach incidents and severity in their organization.

Table 5: Relationship between the uses of risk assessments, network vulnerability scans, and/or penetration tests and security breach incidents

Correlations			
		Security breach incidences	Uses of risk assessments, network vulnerability scans/penetration tests
Security breach incidences	Pearson Correlation	1	.052
	Sig. (2-tailed)		.663
	N	72	72
Uses of risk assessments, network vulnerability scans/penetration tests	Pearson Correlation	.052	1
	Sig. (2-tailed)	.663	
	N	72	72

Source: Research Data (2015)

4.10 Regression Analysis

According to table 22, the correlation co-efficient (R) value was 0.082 with a significant value of

0.926. This indicates that there is a weak relationship between information security policies and security breach incidences ($r<0.5$). However, the relationship among the three variables were not statistically significant ($p>0.05$). As a result, the study fails to reject the fifth null hypothesis and thus concludes that there is no statistical significant relationship between information security policies and security breach incidences. The results reinforce the study of Doherty and Fulford (2005) of no significance statistical significance when they did an exploratory study on information security policies and security breach incidences in organizations in the UK.

The results on table 22 indicate that information security explain only 0.7 percent of the observed security breach incidences as shown by the coefficient of determination (R^2) value of 0.007. The Durbin-Watson that measure autocorrelation was 1.812 and this signifies that there was mo autocorrelation among the independent variables. This is due to the fact that it was within the acceptable levels of 1.5 to 2.5.

Table 6 Linear Regression Analysis

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics					Durbin - Watson
					R Square Change	F Change	df1	df2	Sig. F Change	
1	.082[a]	.007	-.037	.49870	.007	.155	3	68	.926	1.812

a. Predictors: (Constant), Information security policy updates, Industry best practices, Uses of risk assessments

b. Dependent Variable: Security breach incidences

Source: Research Data (2015)

Table 23 results present the overall significance of the model to be 0.926 with an F value of 0.155. The level of significance was higher than 0.05 and this means that information security policies do not show a statistical significant relationship with security breach incidences.

Table 7: ANOVA[a] Test

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	.116	3	.039	.155	.926[b]
	Residual	16.911	68	.249		
	Total	17.027	71			

a. Dependent Variable: Security breach incidences

b. Predictors: (Constant), Information security policy updates, Industry best practices, Uses of risk assessments,

Source: Research Data (2015)

Table 8: Regression Co-efficient

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	1.692	.578		2.929	.005		
	Information security policy updates	.032	.085	.048	.379	.706	.911	1.098
	Industry best practices	-.063	.145	-.056	-.433	.667	.868	1.152
	Uses of risk assessments	.053	.115	.059	.455	.650	.876	1.141

a. Dependent Variable: Security breach incidences

Source: Research Data (2015)

Table 24, results show the computed significant values in relation to information security policy updates (p=0.706), industry best practices (p=0.667) and use of risk assessments, network vulnerability scans/penetration tests (p=0.650) whereby all the independent variables had a p value of greater than 0.05. This means that the variables did not statistically and significantly influence security breach incidences.

The multi-collinearity statistics results indicated none of the Variance of inflation factor was around or equal to .5. Therefore there was no multi-collinearity between the independent variables. This further is supported by the fact that the tolerance values were more than 0.2.

CONCLUSION

The results demonstrated statistically significant 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. 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.

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.