INFORMATION SECURITY POLICY UPDATES 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

The study analyzed the Impact of Information Security Policies on security breach incidences in Kenyan Savings and Credit Cooperatives Societies (SACCOS). 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 dependent variable was incidences of security breaches while the independent variables were investigation of the relationship between information security policy updates (frequency) and information security breach incidents. The results of the study revealed that there is a weak relationship between information security policies and security breach incidences in the SACCOS sector. The study results hope to add to the body of academic knowledge and practitioners in the SACCOS sector where information repository is a resource.

INTRODUCTION

With the evolution of the Internet and networks in organization, there is an immediate need for current security measures and polices to reduce the threats and challenges emerging from new technologies namely software application and network devices (Alshboul, 2010). According to information security breaches survey conducted by PriceWaterhouse Coopers (PWC) in collaboration with InfoSecurity Europe (2013), indicate that the number of security breaches UK firms are encountering continue to increase. The rise in security breaches is mostly witnessed in small businesses which was only the case of large businesses. The companies who are affected experience approximately 50 percent more breaches in 2013 as compared to a year ago. External attacks and inside threats are significant in most organizations. Attackers by outsiders such as criminals, hackers and competitors cause most security breaches in large businesses. An average large business faces a significant attack every few days. Small businesses were not targets of attackers but are also reporting increasing attacks reported in Information Security breaches survey, (2013).

RESULTS AND DISCUSSION

Table 3 shows the gender of respondents. 81.9 percent (59) of the respondents were males, while 18.1 percent (13) were females out of the total of 72 respondents

Table 1: Frequency of Gender

Gender		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	59	81.9	81.9	81.9
	Female	13	18.1	18.1	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

Table 4 displays the age of the respondents. 32 repondents were between the age 20-30 with 44.4 percent, 34 between 31-40 with 47.2 percent, and 6 between age 41-50 with 8.3 percent out of the total of 72 respondents

Table 2: Frequency of Age of Respondents

Age		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-30	32	44.4	44.4	44.4
	31-40	34	47.2	47.2	91.7
	41-50	6	8.3	8.3	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

Table 5 shows the level of education of the respondents. Diploma holders were 20.8 percent (15), Bachelors degree were 65.3 percent (47), Masters were 12.5 percent (9) and 1.4 percent (1) preferred not to answer.

Table 3: Frequency of Education of Respondents

Level of Education		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Diploma	15	20.8	20.8	20.8
	Bachelors degree	47	65.3	65.3	86.1
	Masters	9	12.5	12.5	98.6
	Prefer not to answer	1	1.4	1.4	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

Table 6 shows the number of years the respondents have worked. Those respondents who have worked less than 1 year were 8.3 percent (6), between 1 and 2 years were 9.7 percent (7), between 2 and 3 years were 29.2 percent (21), between 3 and 4 years were 12.5 percent (9), those who have worked more than 4 years were 40.3 percent (29).

Table 4:Frequency of the Number of Years worked

Number of years worked		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1 year	6	8.3	8.3	8.3
	Between 1 and 2 years	7	9.7	9.7	18.1
	Between 2 and 3 years	21	29.2	29.2	47.2
	Between 3 and 4 years	9	12.5	12.5	59.7
	Above 4 years	29	40.3	40.3	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

Table 7 shows the various positions held by the respondents. Chief Information Officer/Director had 22.2 percent (16), Chief Security Officer/Information had 2.8 percent (2), Security Officer 1.4 percent (1), Privacy/Compliance Officer had 2.8 percent (2), Chief Executive Officer had 2.8

percent (2), Technician 2.8 percent (2), Database Administrators had 23.6 percent (17), Network Administrators had 12.5 percent (9), Data Entry Clerk had 1.4 percent (1), Other had 2.8 percent (2), System administrator had 25.0 percent (18).

Table 5: Frequency of Job Title

Job Title		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Chief Information Officer/Director	16	22.2	22.2	22.2
	Chief Security Officer/Information	2	2.8	2.8	25.0
	Security Officer	1	1.4	1.4	26.4
	Privacy/Compliance Officer	2	2.8	2.8	29.2
	Chief Executive Officer	2	2.8	2.8	31.9
	Technician	2	2.8	2.8	34.7
	Database Administrator	17	23.6	23.6	58.3
	Network Administrator	9	12.5	12.5	70.8
	Data Entry Clerk	1	1.4	1.4	72.2
	Other	2	2.8	2.8	75.0
	System administrator	18	25.0	25.0	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

Respondents were asked to state the privacy or security law their SACCOS complied with. Table 8 presents the results whereby 80.6 percent (58) respondents said their SACCOS complied with The Data Protection Bill 2012, those who complied with the Kenya Law Reform were 2.8 percent (2), 6.9 percent (5) indicated that their SACCOS complied with PIPEDA, 9.7 (7) indicated that they did not Know the privacy or security Law their SACCOS complied with.

Table 6: Frequency of Privacy or Security Law Complied With

Privacy/Security Law		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	The Data Protection Bill 2012	58	80.6	80.6	80.6
	Kenya Law Reform Commission	2	2.8	2.8	83.3
	PIPEDA	5	6.9	6.9	90.3
	Do not know	7	9.7	9.7	100.0
	Total	72	100.0	100.0	

Source: Research Data (2015)

4.4 Security Breach Incidences

Under security breach incidences, respondents were asked to indicate an approximate number of occurrences of security threats reported by their SACCOS in the last two years. Table 9 indicates that 18.1 percent (13) reported that they have not been attacked by a Computer Virus, 55.6 percent (40) indicated that they have been affected by a Computer virus with an occurrence from 1 to 5 times, 20.8 percent (15) said that they have been affected by a Computer virus from 6 to 10 times, 5.6 percent (4) indicated that they have been affected by a Computer virus from 11 to 14 times and no SACCOS reported a computer viruses greater than 14 times. Computer viruses had a mean of 2.19 and a standard deviation of 0.929.

The results for Hacking incident (external) shows that 91.7 percent (66) indicated that they have not been hacked externally. 8.3 percent (6) have been hacked externally from 1 to 5 occurrences; from 6 to 10, 11 to 14 and greater than 14 occurrences have not been hacked externally. Hacking incident (external) mean is 1.08 and a standard deviation of 0.278.

Under unauthorized access to/use of data (internal), 68.1 percent (49) have not had their internal employees access or use data without authorization, 29.2 percent (21) have had their internal employees access or use data without authorization from 1 to 5 times, 2.8 percent (2) have had their internal employees access or use data without authorization from 6 to 10 times. Occurrences from 11 to 14 and greater than 14 have not recorded any violations of unauthorized access or use of data by their internal employees. Unauthorized access to or use of data internally had a mean of 1.35 and a standard deviation of 0.535.

Table 7: Security Threats Occurrences in the Last two Years

Type of Breach	Security Breach Incidences						
	0	1-5	6-10	11-14	>14	Mean	Std Deviation
Computer virus	18.1% 13	55.6% 40	20.8% 15	5.6% 4	0% 0	2.19	0.929
Hacking incident (external)	91.7% 66	8.3% 6	0% 0	0% 0	0% 0	1.08	0.278
Unauthorized access to / use of data (internal)	68.1% 49	29.2% 21	2.8% 2	0% 0	0% 0	1.35	0.535
Theft of hardware / software	77.8% 56	20.8% 15	1.4% 1	0% 0	0% 0	1.24	0.459
Computer-based fraud	61.1% 44	36.1% 26	2.8% 2	0% 0	0% 0	1.42	0.550
Human error	36.1% 26	36.1% 26	20.8% 15	1.4% 1	5.6% 4	2.04	1.067
Natural disaster	68.1% 62	29.2% 9	2.8% 1	0% 0	0% 0	1.15	0.399
Damage by disgruntled employee	93.1% 67	4.2% 3	2.8% 2	0% 0	0% 0	1.10	0.381

Source: Research Data (2015)

When the respondents were asked about the theft of hardware and/or software, 77.8 percent (56) reported that they had not recorded any theft, 20.8 percent (15) had recorded theft from 1 to 5 occurrences, 1.4 percent (1) recorded occurrence from 6 to 10 times, from 11 to 14 and greater than 14 times had not recorded any incidents in their last two years. A mean of 1.24 and a standard deviation of 0.535 were achieved.

Computer-based fraud results indicated that 61.1 percent (44) repondents had not experienced Computer-based fraud, 36.1 percent (26) had an occurrence from 1 to 5 times, 2.8 percent (2) had recorded an occurrence from 6 to 10 times, and none had recorded Computer-based fraud occurrences from 11 to 14 and greater than 14 times. Computer-based fraud had a mean of 1.42 and a standard deviation of 0.550.

Under human error, 36.1 percent (26) of the respondents indicated that they had not recorded any incident. The same 36.1 percent (26) was recorded 1 to 5 times. 20.8 percent (15) reported occurrences from 6 to 10 times, 1.4 percent (1) reported an occurrence from11 to 14 and 5.6 percent (4) reported an occurrence greater than 14 times. Human error had a mean of 2.04 and a standard deviation of 1.067. This indicates that human error is a critical type of breach to most SACCOS.

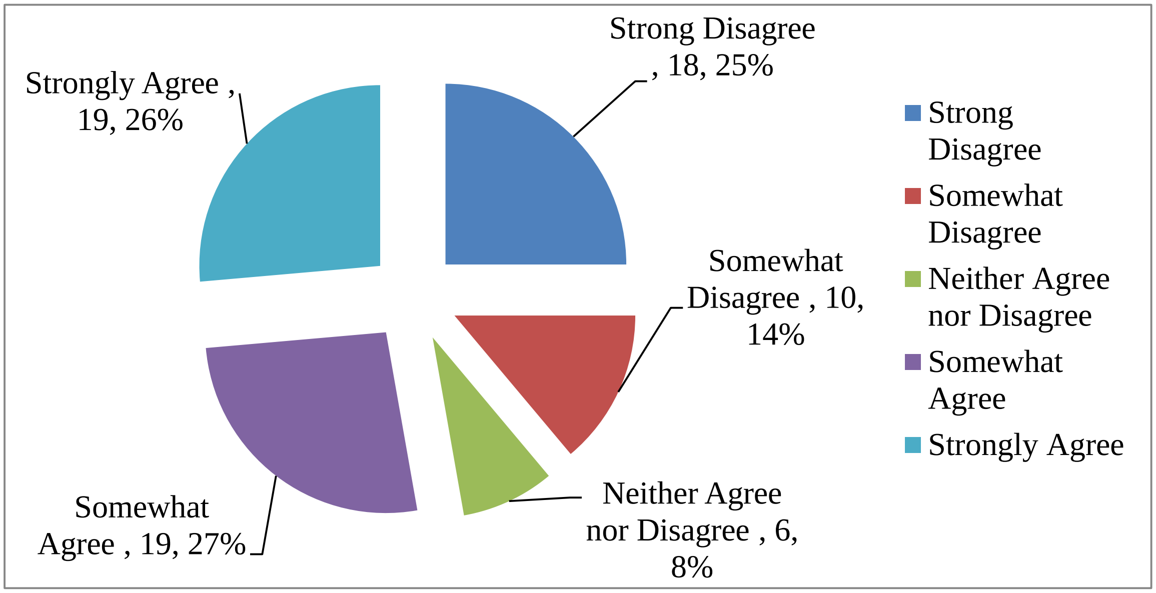
The results of natural disaster had 68.1 percent (62) of their respondents had not recorded any occurrences, 29.2 percent (9) had reported the occurrence from 1 to 5 times, 2.8 percent (1) had reported an occurrence from 6 to 10 times, from 11 times or more had not reported any occurrences of natural disaster. A mean of 1.15 and standard deviation of 0.399 was obtained.

Under damage by disgruntled employee, 93.1 percent (67) reported no occurrence, 4.2 percent (3) reported an occurrence from 1 to 5 times, 2.8 percent (2), from 11 and more occurrences reported no security breach incident. A mean of 1.10 and standard deviation of 0.381 was obtained from damage by disgruntled employee.

4.5 Information Security Policies Updates

Figure 2 presents the results of SACCOS written IT security policies. The results indicate if IT security policies were created as a result of security incident/breach. 25 percent (18) strongly disagree, 13.9 percent (10) somewhat disagree, 8.3 percent (6) neither agree nor disagree, 26.4 percent (19) somewhat agree and strongly agree. The results indicate that 26.4 percent of the SACCOS in the study created their IT security policies as a result of a security incident/breach.

Figure 1: Written IT Policies



Source: Research Data (2015)

When asked about documentation of IT security policies, table 10 present the result set forth. 2.8 percent (2) have not documented their IT security policies, 69.4 percent (50) takes years to document their IT security policies, 23.6 percent (17) takes months to document their IT security policy and 4.2 percent (3) did not know if their IT security policy was documented.

Table 8: Documentation of IT Security Policies

Documentation of IT security policies	**Frequency**	**Percentage**	**Cumulative Percentage**
Never	2	2.8	2.8
Years	50	69.4	72.2
Do not know	3	4.2	76.4
Months	17	23.6	100
Weeks	0	0	

Source: Research Data (2015)

Respondent were asked how often IT security policy gets updated. Table 11 present the result as follows 2.8 percent (2) do not update their IT security policies, 27.8 percent (20) updates every two years, 56.9 percent (41) updates every year 9.7 percent (7) updates less than one year and 2.8 percent (2) did not know.

Table 9: Frequency of IT Security Policy Updates

IT Security Policies Updated	Frequency	Percentage	Cumulative Percentage
Never	2	2.8	2.8
Every 2 years	20	27.8	30.6
Do not know	2	2.8	33.4
Every year	41	56.9	90.3
Less than 1 year	7	9.7	100

Source: Research Data (2015)

In testing the hypotheses, Bivariate Correlations was employed. The correlation test revealed the results of the relationship between information security policy updates (frequency) and information security breach incidents as indicated on table 18. There is no statistical significant relationship between information security policy updates and security breach incidences because the r value is 0.048 and a p value of 0.692 therefore the study accepts the null hypothesis. This means that SACCOS registered with SASRA need to reinforce their information security policy updates to curb the issue of security breach incidents and severity

Table 10: Relationship between information security policies updates (frequency) and information security breach incidences

Correlations			
.		Security breach incidences	Information security policies updates
Security breach incidences	Pearson Correlation	1	.048
	Sig. (2-tailed)		.692
	N	72	72
Information security policy updates	Pearson Correlation	.048	1
	Sig. (2-tailed)	.692	
	N	72	72

Source: Research Data (2015)

Table 19 presents the results of the relationship between industry best practices and information security breach incidents. The r value is -0.026 and p-value is 0.831 indicating there is no statistical significance between the variables. The study as a result accepts the null hypothesis. Based on the results it is important for SACCOS to reinforce the use of best practices in running their operations.

CONCLUSION

The study results demonstrated no evidence of a statistically significant relationship between information security policy updates (frequency) and information security breach incidents within SACCOS. This finding reinforces Doherty and Fulford (2005) findings of no significance statistical significance when they did an exploratory study on organizations in the UK. SACCOS' respondent results indicated that when IT security policies were updated less often, incidence of computer viruses increased. The results demonstrated a significant but weak relationship in this regard among the respondent SACCOS. Further research is required to determine whether this increased incidence of computer viruses is attributable to a failure by SACCOS to update their information security policies as necessary to reduce the number of computer viruses with the SACCOS sector.

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.