THE INTERNATIONAL JOURNAL OF BUSINESS & MANAGEMENT

A Model for Assessing Security Risk Exposure in Savings and Credit Cooperative Societies

Joshua KiprotichMutai
Ph.D. Student, School of Computer Science and Bioinformatics, Kabarak University, Kenya
Nelson Bogomba Masese
Senior Lecturer, School of Computer Science and Bioinformatics, Kabarak University, Kenya

Abstract:
Breaches of security in Savings and credit cooperative societies (SACCOs) continue to take an upward trend as reports indicate that these organizations continue to position themselves to fully adopt Information and communication technologies to assist in performing back-end operations more effectively. As report further indicate, these SACCOs still lack behind their counterparts in mainstream banking sector as far as investments towards mitigation of security risks are concerned. The SACCO industry therefore is exposed to security threats. In order to reduce these exposures to security threats in SACCOs, there needs to be mechanisms through which these organizations can assess their posture as regards to how exposed they are and what actions they need to apply. This research offers a solution by developing a model for computing the security risk exposure index (SREI). A descriptive research design was used in this study where the target population was 50 respondents. Structured questionnaires were used in the study to collect quantitative primary data which the researcher analyzed using both descriptive and inferential statistics. Descriptive statistics, on one hand, used frequencies and percentages while inferential statistics, on the other hand, was used to analyze the correlation between the independent variables and the dependent variable (SREI). The study established six out of eleven ISO 27001 cardinal control factors were most critical to SACCOs. The study established a negative correlation between each of the six factors and the dependent variable. Therefore, this study recommends the use of the Security risk exposure index (SREI) model to indicate exposure in SACCOs and recommend appropriate actions to achieve security risk maturity.

Keywords: *Model, ISO27001 factors, Security Risk Exposure Index*

1. Background

Savings and credit cooperative societies are a subset of a wider world cooperative movement which can basically be defined as independent alliance of people who willingly unite to uplift their social, cultural, and economic desires through commonly-owned and democratically-controlled endeavor (ICA, 2005). This industry is continually growing in Kenya with government records indicating immense increase in assets that deposit-taking SACCOs possess. For instance, the aggregate total of assets grew by 13.7 percent between 2014 and 2015. These totals are expected to grow even larger in future (SASRA, 2015a).

Besides the government's requirement for deposit-taking SACCOs to computerize their backend operations, the immense growth, competition and need for improved efficiency in delivering services to customers necessitates them to do so (Chahayo et al., 2013). Research further indicates that the adoption of e-banking services by deposit-taking microfinance institutions is increasing as many of them begin to embrace technology (Atavachi, 2013).

As the growth in adoption of ICTs in Kenya is being recorded, the threat landscape continues to climb on the cyberspace (Bauer & Dutton, 2015). Every business that is connected to the internet has the propensity of falling victim to cyber-crime at some point in time because cyber criminals are expanding their ability of stealing money directly or turning stolen data into money (Nyawanga, 2015). Banks and other financial institutions remain prime targets of cyber criminals (Maina, 2017). According to Kigen et al. (2015), SACCOs, unlike banks lack skilled security personnel and anti-fraud systems to avert cybercriminals.

1.1. Statement of the Problem

SACCOs in Kenya are notably racing towards adoption of ICTs to assist in driving their backend operations. This is probably due to present government regulations, competition with banks and other microfinance institutions, and need for efficient delivery of services to their customers. Consequently, increased aggregates in total assets that SACCOs possess continue to be recorded. It is noted that middle level financial institutions which include SACCOs and Microfinance institutions focus their investment on customer satisfaction and mechanisms of reducing operating costs and therefore tend to disregard necessary investment towards security controls for their assets. In the midst of climbing threat landscape on the cyberspace, financial sector continue to record increased security breaches with worrying statistics indicating that Kenyan SACCOs lost 2Billion Shilling to cybercrime in 2016 alone. It is therefore necessary to enforce sufficient controls. To do so, there is need to design a model riding on international standards for information security,

which will help SACCOs to determine their security exposure level and provide appropriate recommendations to help the organizations to carry out their businesses in a safe cyberspace.

1.2. Objective of the Study

To design the model for computing security risk exposure index of savings and credit cooperative in Kenya.

2. Literature Review

2.1. Conceptual Framework

The research study derived a formula for computing security risk exposure index (SREI). The conceptual framework for derivation of the formula for computing SREI is presented in figure 1. While the independent variables of the model are basically the ISO/IEC 27001 standard controls, the dependent variable is the function of all the independent variables. Government regulations form the moderating variables.

SREI=f (Security Policy, Human Resource Security, Organization of Information Security, Asset Management, Physical and Environmental Security, Communications and Operations, Access Control, Information Security Incident Management, System Security, Business Continuity Management, Compliance)

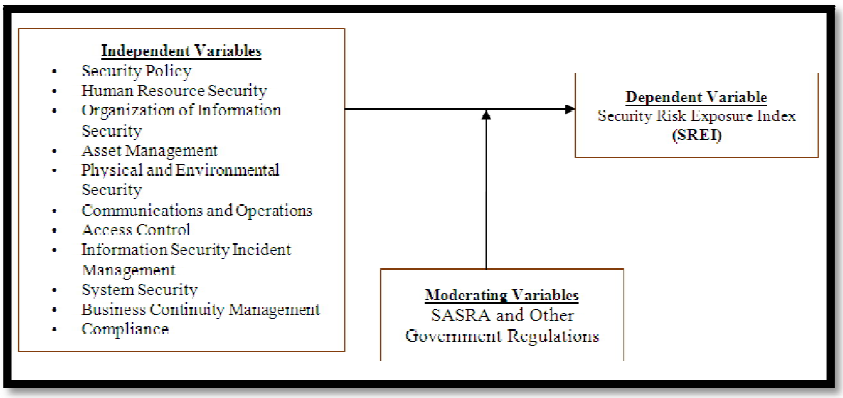

Figure 1: Conceptual Framework

2.1.1. Design and Formulation of the Model

The Security Risk Exposure Index (SREI) was computed as a function of weight and security variable scores and implemented as a mathematical model demonstrated by the formula shown below;

$SREI=W_1V_1+ W_2V_2+ W_3V_3+ \ldots\ldots\ldots\ldots\ldots\ldots + W_nV_n$

Equation 1: Model Equation

Where;

$W_1, W_2, W_3 \ldots\ldots\ldots\ldots\ldots\ldots W_n$ respectively, are different weights that were to be determined from a cross-section of the multiple case results discussed in the study.

While;

$V_1, V_2, V_3 \ldots\ldots\ldots\ldots\ldots\ldots V_n$ respectively, are security variables associated with security risk exposures for which in the case of this study are the security checklist components of all the ISO/IEC 27001 security controls for the independent variables. Computation of SREI sought to manage these parameters. On the overall, the model was to compute SREI by comparing SACCO's security posture against thresholds of ISO 27001 best practices. The scores below the threshold were supposed to place the SACCO's security status as wanting. Cases below the threshold values were to trigger actions alerts, for instance, pinpointing security control gaps that need to be filled, and disciplinary action by the regulating authorities.

2.1.2. Model Metrics

To obtain Security Risk exposure index (SREI) of an organization, Risk assessment questions were asked where respondents were to answer in a scale of 1 to 5 whereby 1 meant that the respondent was strongly disagreeing to assessment statement while 5 meant that the respondent was strongly agreeing to the assessment statements. In the same tone, the other responses included; Disagree, Neutral and Agree.

The scores of the respondent per assessment question denoted the level of compliance to ISO27001 standard by the respondent and associated organization which in this case was referred to as Security maturity factor of the organization (Y). The following linear regression modeling equation was used to compute weights necessary for computing Security maturity factor (Y) and by extension the Security Risk Exposure Index (SREI).

$Y= W_1V_1 + W_2V_2 \ldots + W_nV_n$

Where

Y = Security Maturity factor of the organization
W = Weights
V = Security Variable (User assessment Score per question)
n = Number of assessment questions

Suppose all the assessment questions have constant coefficients, such that $W=W_1=W_2=\ldots W$,

Then, the weight will be W, whereby
$Y = W V_1+WV_2+WV_3+...WV_n$.
Since W is common,
$Y= W (V_1+V_2+V_3+ ...Vn)$
Equation 1: Mathematical Maturity Model
In the case of the this study, there were **n** number of questions that were used for Security Risk Assessment, in which case, n=40 and the maximum score that the user could have in a scale of 1 to 5 was; 5*n = 5n.
If we put back this to maturity equation 4 above, then;

$$Y = \frac{V1}{5n} + \frac{V2}{5n} + \frac{V3}{5n} + \dots \frac{Vn}{5n}$$

Therefore;

$$Y = \frac{1}{5n}(V1 + V2 + V3 + \dots Vn)$$

Hence

$$W = \frac{1}{5n}$$

In the view of the above, the relevant weight for the SREI model based on n Assessment questions was $\frac{1}{5n}$;
The value of maturity factor Y could be represented as a percentage factor (Y %) as shown in equation 5 below;

$$Y = \frac{1}{5n}(V1 + V2 + V3 + \dots Vn) * 100$$

Hence

$$Y = \frac{20}{n}(V1 + V2 + V3 + \dots Vn)\%$$

Equation 2: Percentage Maturity Factor

2.1.3. SREI Mathematical Model

By achieving the weight and the maturity model of the organization, which denotes the level of compliance to the ISO27001 standard, as shown in equation 5 above, SREI was computed as a level of immaturity or non-compliance to ISO27001 standard. SREI basically represented the gap between full compliance to ISO27001 standard and the actual posture of the organization represented by the maturity score. The equation for computing SREI as a percentage factor was therefore derived as follows;
$SREI = 100 - Y\%$
Since Y% was already derived in equation 5, then by substitution, the complete percentage SREI equation was a shown in equation 6 below;

$$SREI = 100 - \left\{\frac{20}{n}(V1 + V2 + V3 + \dots Vn)\right\}$$

Equation 3: SREI Mathematical Model

2.2. Model Scenarios

The Security Risk exposure Index of an organization was determined by first maturity factor of the organization as shown in equation 2 which represented the compliance level of the organization to ISO27001 standard, and second computing SREI as shown in equation 3 which represents the organizations deficit score or gap for it to attain full compliance to ISO27001 standard. There are therefore three model scenarios which are explained in sections 4.5.1 to 4.5.3, namely; Best case scenario, Average case scenario, and Worst case scenario.

2.2.1. Best Case Scenario

Suppose the total assessment questions for all the ISO/IEC 27001 controls, then n=40, the best case scenario is achieved when sum of assessee's scores for the 40 risk assessment questions.
That is $V1 + V2 + V3 + \cdots V40 = 200$
By substituting back to equation 2,

$$Y = \frac{20}{40}(200) = 100\%;$$

Equation 4: Best case scenario maturity factor
By substituting back to equation 3,
$SREI = 100 - \{0.5(200)\} = 0\%;$
Equation 5: Best case scenario SREI
Equations 4 and 5 above depicts that the user and their organization are fully compliant to the specific requirements of ISO27001 standard at Y=100% and that it is Least exposed at SREI = 0%.

2.2.2. Average Case Scenario

The average case scenario is the middle position whereby the organization is 50% exposed and 50% mature. In a scale of 1 to 5, which was the case in this study, the average case scenario is where the assessee scored an average of 2.5 per question or total score of 100 for the 40 assessment questions which tends towards a neutral score. This implies that

the organization is neutral and can neither be fully compliant to ISO27001 requirements nor fully exposed. The following equations 6 and 7 presents the maturity and exposure factors for the average case scenarios respectively.

$Y = 0.5(100) = 50\%$;

Equation 6: Average case scenario maturity score

$SREI = 100 - \{0.5(100)\} = 50\%$

Equation 7: Average case scenario SREI

2.2.3. Worst Case Scenario

The worst case scenario is the converse of the best case scenario whereby the assessment scores depict that the user and their organization are least mature in terms of compliance to specific requirements to ISO27001 standard whereforeY → 0%. This also imply the organization is much exposed with their SREI tending towards 100%; that is, SREI → 100%.

When scores in a scale of 1 to 5 are used as was the case in this study, the worst case scenario is attained when the assessee attains an average of 1 per question or a sum of 40 for all the 40 assessment questions. Therefore the worst case scenario values for maturity factor and exposure factor are presented in equations 8 and 9 respectively.

$Y = 0.5(40) = 20\%$;

Equation 8: Worst case scenario maturity factor

$SREI = 100 - \{0.5(40)\} = 80\%$;

Equation 9: Worst case scenario SREI

2.2.4. Threshold Scores and Assessment Scale

According to SREI model, the threshold scores which are in a scale of 1 to 5 were pegged at 4. This score denotes that the assessee agrees to be compliant to the requirements of ISO27001 standard. Score 5, which denote that the assessee is in strong agreement with the issue of compliance with ISO27001 standard requirements. This meant that the assessee's average score per assessment question was at a mature 5 and therefore the least exposure factor. However, average scores of 1, 2 and 3 which are below the threshold score (4) means that the user's exposure index is increasingly tending towards 80% which is considered to be highly risky case for the organization. These scenarios therefore call for action by the organization to minimize the risk. Recommendations for best practices are therefore pegged on these threshold scores.

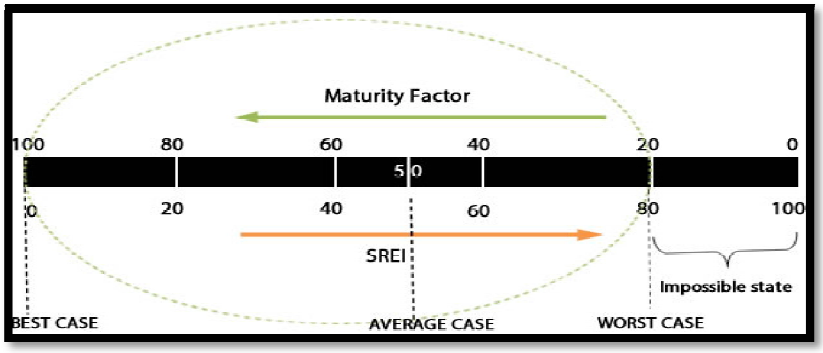

Figure 1: Assessment Scale
Source: Researcher (2018)

As presented in the equations 8 and 9 above, the worst case scenario is represented by 20% maturity and 80% exposure factors respectively. The 0% maturity and 100 exposure factors cannot be computed from the model because the model computation for these factors is pegged on a scale of 1 to 5 which yields the said results. This is called the impossible state as shown in the figure 2.

3. Research Design

This study was carried out on all the eleven SASRA-licensed deposit-taking SACCOs operating within Nakuru central business district. The SACCOs had ICT infrastructure and systems in place which was a requirement by SASRA for licenses and therefore were fit for the study additionally, the SACCOs comprised of a wide spread based on major customer types they serve, namely, teachers, farmers, workers, community and business. A purposive sampling technique was used to get five respondents from each SACCO who included; branch manager, ICT manager, system administrator, database administrator and operations manager. Therefore the sample size of 55 was used in the study. The study collected largely quantitative primary data using semi-structured questionnaires as instruments for the study. The questionnaires were administered to the respondents on drop-and-pick method and the collected data as analyzed using descriptive statistics.

4. Results

The respondents were required to provide their view on how they think the 11 ISO 27001 control factors were critical or not critical to their SACCO. The results are presented in table 1 below;

Statement	NVC	NC	N	C	VC
Ratings	Freq (%)	Freq (%)	Freq (%)	Freq (%)	Freq (%)
Security Policy	20(40)	30(60)	0(0)	0(0)	0(0)
Physical and Environmental Security	0(0)	0(0)	0(0)	15(30)	35(70)
Human Resource Security	0(0)	5(10)	3(6)	15(30)	27(54)
Asset Management	0(0)	0(0)	0(0)	8(16)	42(84)
Communication Management & Operations Management	4(8)	40(80)	6(12)	0(0)	0(0)
Organization of Information Security	18(36)	32(64)	0(0)	0(0)	0(0)
System Security	0(0)	3(6)	4(8)	18(36)	25(50)
Access Control	1(2)	6(12)	1(2)	19(38)	23(46)
Information Security Incident Management	16(32)	30(60)	4(8)	0(0)	0(0)
Business Continuity Management	16(32)	34(68)	0(0)	0(0)	0(0)
Compliance	0(0)	5(10)	5(10)	0(0)	40(80)

Table 1: Critical Nature of ISO 27001 Security Risk Factors In Saccos
Key: NVC=Not Very Critical, NC= Not Critical, N=Neutral, C=Critical, VC=Very Critical, Freq=Frequency, and%=Percentages
Source: Research Data (2018)

The results depicted that the security risk factors that were considered to be very critical or critical (VC%,C%) to SACCO included; Physical and Environmental Security (70%,30%), Human Resource Security (54%,30%), Asset security and management (84%,16%), System Security (50%,36%), Access Control (46%,38%), and Compliance (80%,0%). However, the respondents consider the following risk factors to be not very critical or not critical (NVC%, NC %); Security policy (60%, 40%); communications & Operations Management (8%, 80%); Organization of Information Security (36%, 64%); Business Continuity Management (32%, 68%); and Information Security Incident Management (32%, 60%) were considered as not critical.

4.1. Correlation Analysis

A correlation analyses was carried out to determine whether there exist a relationship between independent variables (Each of the six ISO27001 factors) and dependent variable (SREI) of the study. On one hand, the values for the each independent variable needed for performing correlation were obtained by getting a cumulative sum of all scores from respondents for the sub-variables within that variable. On the other hand, the values for independent variable (SREI) were obtained through computation using SREI formula.

$$SREI = \{1 - 0.005(V1 + V2 + \cdots V40)\} * 100$$

The summary of the source data that was used for correlation is shown in appendix E. The following subsequent sections; 4.1.1 to 4.1.6 shows the analysis of the findings using Pearson's correlation between SREI and cumulative sum of independent variables per respondent.

4.1.1. Correlations between Security Risk Exposure Index and Asset Security

		Security Risk Exposure Index	Asset Security
Security risk exposure index	Pearson Correlation	1	-.477**
	Sig. (2-tailed)		.000
	N	50	50
Asset security	Pearson Correlation	-.477**	1
	Sig. (2-tailed)	.000	
	N	50	50
**. Correlation is significant at the 0.01 level (2-tailed).			

Table 1: Correlation between SREI and Asset Security

The findings revealed that there exists a strong negative and statistically significant relationship between security risk exposure index and asset security ($r=-0.477^{**}p<0.01$). This means that when factors relating to asset security increases it leads to a decrease in Security Risk Exposure Index.

4.1.2. Correlations between Security Risk Exposure Index and Physical and Environmental Security

		Security Risk Exposure Index	Physical And Environmental Security
Security risk exposure index	Pearson Correlation	1	-.185
	Sig. (2-tailed)		.199
	N	50	50
Physical and environmental security	Pearson Correlation	-.185	1
	Sig. (2-tailed)	.199	
	N	50	50

Table 2: Correlations between SREI and Physical and Environmental Security

The findings revealed that there exists a negative and statistically significant relationship between security risk exposure index and Physical and Environmental Security (r=-0.185p). This implies that increase in Physical and Environmental Security will decrease security risk exposure index of the organization.

4.1.3. Correlations between Security Risk Exposure Index and System Security

		Security Risk Exposure Index	System Security
Security risk exposure index	Pearson Correlation	1	-.737**
	Sig. (2-tailed)		.000
	N	50	50
System security	Pearson Correlation	-.737**	1
	Sig. (2-tailed)	.000	
	N	50	50
**. Correlation is significant at the 0.01 level (2-tailed).			

Table 3: Correlations between SREI and System Security

The findings of the analyzed data point out that there exist a strong negative and statistically significant relationship between Security Risk Exposure Index and System Security (r=-0.737**p<0.01). This means that as the system security increases, security risk exposure index decreases and vice versa.

4.1.4. Correlations between Security Risk Exposure Index and Human Resource Security

		Security Risk Exposure Index	Human Resource Security
Security risk exposure index	Pearson Correlation	1	-.665**
	Sig. (2-tailed)		.000
	N	50	50
Human resource security	Pearson Correlation	-.665**	1
	Sig. (2-tailed)	.000	
	N	50	50
**. Correlation is significant at the 0.01 level (2-tailed).			

Table 4: Correlations between SREI and Human Resource Security

The findings revealed that there exist a negative and significant relationship between Security Risk Exposure Index and human resource security (r=-0.665**p<0.01). This implies that as human resource security increase, security risk exposure reduce and vice versa.

4.1.5. Correlations between Security Risk Exposure Index and Access Controls

		Security risk exposure index	Access control
Security risk exposure index	Pearson Correlation	1	-.711**
	Sig. (2-tailed)		.000
	N	50	50
Access control	Pearson Correlation	-.711**	1
	Sig. (2-tailed)	.000	
	N	50	50

Table 5: Correlations between SREI and Access Controls
***. Correlation is significant at the 0.01 level (2-tailed)*

The findings pointed that there exist a negative and statistically significant relationship between Security Risk Exposure Index and Access Controls ($r=-0.711^{**}$; $p<0.01$). This infers that, when access control is improved; the security risk exposure index will decrease and vice versa.

4.1.6. Correlations between Security Risk Exposure Index and Compliance

		Security Risk Exposure Index	Compliance
Security risk exposure index	Pearson Correlation	1	-.732**
	Sig. (2-tailed)		.000
	N	50	50
Compliance	Pearson Correlation	-.732**	1
	Sig. (2-tailed)	.000	
	N	50	50

Table 6: Correlations between SREI and Compliance

***. Correlation Is Significant at the 0.01 Level (2-Tailed)*

The findings of the data analyzed disclosed that there exist a strong negative and statistically significant relationship between Security Risk Exposure Index and Compliance ($r=-0.732^{**}$; $p<0.01$). This implies that every aspect of compliance when enhanced will decrease the security risk exposure index in the organization.

5. Conclusions

The study established that the most critical security risk factors affecting Savings and Credit Cooperative Societies in Kenya from the 11 of ISO27001 factors are; physical and environmental security, Human Resource security, asset management and security, system security, access control, and compliance. These factors contributed the most to the exposure of SACCOs to security threats. Although the SACCOs in Kenya were required to pay attention to all the 11 ISO27001 control factors, more attention needed to be put on the 6 factors established by this study if minimum exposure index was to be realized. Therefore the SREI system was necessary in helping the SACCOs to establish their exposure index and recommended controls to secure their organizations. In addition all the six ISO 27001 factor that are most critical to SACCOs presented a negative correlation to SREI which implies that as the level of implementation of these specific elements by SACCOs increase, the SREI factor decrease and vice versa.

6. Recommendations

This study recommends enforced compliance. SACCO Societies Regulatory Authority (SASRA) should incorporate this model in their oversight role of the SACCOs in Kenya. SASRA can enforce the requirement for SACCOs to perform their online security risk assessments on monthly basis alongside other regulatory reports they receive monthly from licensed SACCOs. This will help monitor the improvement or non-improvement of SACCOs in compliance with ISO 27001 standard requirements for security.

7. References

i. Atavachi, B. S. (2013). Effect of electronic banking on financial performance of deposit taking micro-finance institutions in Kenya (Doctoral dissertation, University of Nairobi).

ii. Bauer, J. M., & Dutton, W. H. (2015). The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet.

iii. Chahayo, S. A., Bureti, F., & Juma, M. M. and Aketch RA (2013). Analysis of Financial Mismatch in Co-Operative Societies: A Case of Kakamega County, Kenya. International Journal for Management Science and Technology, 1(5).

iv. Fomin, V. V., Vries, H., & Barlette, Y. (2008, September). ISO/IEC 27001 information systems security management standard: Exploring the reasons for low adoption. In Proceedings of the third European conference on Management of Technology (EuroMOT).

v. Guguyu, O. (2016). Kenya: Central Bank Puts Firms on High Alert Over Cyber Attacks. allAfrica.com. Retrieved 6 April 2017, from http://allafrica.com/stories/201605251074.html

vi. ICA. (2005). International Cooperative Alliance Statement of the Co-operative identity, values & principles. http://old.ica.coop/en/whats-co-op/co-operative-identity-values-principles.

vii. Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., ... & Shitanda, S. (2015). Kenya Cyber Security Report 2015. Serianu Limited.

viii. Kigen, P. M., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Ndegwa, D., ... & Shitanda, S. (2016). Kenya Cyber Security Report 2016. Serianu Limited.

ix. Maina, S. (2017). REPORT: African Countries Lost At Least 2 Billion Dollars to Cyberattacks in 2016. Techweez. Retrieved 18 March 2017, from http://www.techweez.com/2017/04/11/africa-cyberattacks-reports-2016/

x. Nyawanga, J. O. (2015). Meeting the challenge of cyber threats in emerging electronic transaction technologies in in Kenyan banking sector (Doctoral dissertation, University of Nairobi).

xi. Project Sonar by Rapid7. (2017). Sonar.labs.rapid7.com. Retrieved 7 April 2017, from https://sonar.labs.rapid7.com/

xii. Rudis, B., Beardsley, T., & Harts, J. (2017). Security Research: National Exposure Index. Rapid7. Retrieved 5 April 2017, from https://information.rapid7.com/national-exposure-index.html
xiii. SACCO Societies Regulatory Authority (SASRA). (2015a). Sacco Supervision Report:
xiv. Deposit Taking SACCOs. In house Publication.
xv. SACCO Societies Regulatory Authority (SASRA). (2015b). Guideline on Risk Management Practices for Deposit Taking SACCOs. In house Publication.
xvi. Schweizerische, S. N. V. (2013). Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization.
xvii. Wechuli, N. A., Franklin, W., & Jotham, W. (2017). Cyber Security Challenges to Mobile Banking in SACCOs in Kenya. International Journal of Computer (IJC), 27(1), 133-140.