
Antone Muga Otieno, Susan Were, Makori Moronge

1 Student, Jomo Kenyatta University of Agriculture & Technology, Nairobi, Kenya
2 Lecturer, Jomo Kenyatta University of Agriculture & Technology, Nairobi, Kenya
3 Lecturer, Jomo Kenyatta University of Agriculture & Technology, Nairobi, Kenya

Abstract: The growth of the internet has affected lives of many people either positively or negatively. It has enabled the exchange of information promptly which has brought a lot of benefits in the areas of commerce, education and social interactions but on the contrary it has provided an opportunity for the offenders to commit large crimes costing huge sums of money. The study aims to analyze the influence of cyber security strategy on online consumer protection in Kenya. It focuses on two major online shops in Kenya, Jumia and OLX. It examines how the four variables; Cyber security governance, Cyber security research and development, Cyber Space Legal and Regulatory Frameworks and Cyber Security Infrastructure affects the protection of online consumers in Kenya.

Keywords: online consumers, Cyber security, governance, research and development, Regulatory Frameworks, Infrastructure

1. Introduction

Computer systems related crimes have existed since 1940s and 1950s when the computers were invented and by then there were no computer crime laws prohibiting activities that caused harm. Magutu, Ondimu and Ipu, (2011) with the interconnection of more computers to form the internet, computer systems abuses became on the rise forcing the federal and state governments to formulate computer crime laws. According to national cyber security strategy by Government of Kenya (GoK), cybercrimes are evolving faster than the cyber defenses and this has resulted in the increase on the attacks levels making it a big threat. The attacks usually involve the use of sophisticated techniques but also low penetration like insider threats also poses a great challenge to organizations.

According to Magutu et al., (2011) Kenyan online consumers and SMEs have showed slow or non-adoption of existing cyber security strategies; however the GoK has come up with four strategic goals to ensure cyber security among businesses. Firstly by enhancing national security posture through protection of information infrastructure, secondly, creating cyber security governance to ensure safe cyber space, thirdly, improving on information sharing among various stakeholders and lastly defining objectives and goals of cyber security and implementation from the national level. (GoK, 2014)

2. Local perspective of cyber security strategies

According to Communications Authority of Kenya, formerly CCK internet usage in Kenya was estimated to 21.2 million up from 19.1 million in the statistics annual report for the year 2014-2015. With the increase in internet usage, there has equally been an upward trend in cyber insecurity which has cost the country more than 2 billion Kenya shillings (US$ 22.56 million) in 2013 (Ignio & Nanjira., 2015). Kenyan Internet service Providers (ISPs) have got poor spamming reputation scores Serianu (2012). This exposes users to risks of losing their data and even possibility of being an easy target of fraud. Many Kenyan computers are attacked by botnets, viruses, Trojans and worms because of poor or non-implementation of cyber security strategies kimwele, Mwangi and Kimani (2005). Botnets families detected in Kenya according to Serianu in cyber security report of 2012 include; Torping, Grum, Waledac, Lethic, Cutwail and Bobax.

Kenya ranks 7th position in Africa with South Africa at top on internet security threats. Kenyan banks lost 3 billion shillings ($ 24 million) due to identity theft, illicit fund transfers and credit card fraud Delloite, (2010). The Communications Authority of Kenya in the white paper on E commerce adoption in Kenya 2015, estimated the value of e-commerce in Kenya in 2012 to have grown to USD50 million or...
approximately USD1.2 per head of the population. The current Kenyan cyber-crime and computer related bill of 2014 does not extensively address e-consumer privacy, ICT legislation and e-security amongst others hence leaving the consumers more prone to abuses by both the hackers and rogue e-suppliers.

3. Objectives of the Study

3.1 General objective

To determine the influence of cyber security strategies on online consumer protection in Kenya, a case study of OLX and Jumia.

3.2 Specific objectives

i) To evaluate the effect of cyber security governance on online consumer protection in Kenya.

ii) To re-affirm the influence of Cyber security research and development on online consumer protection in Kenya.

iii) To establish the influence of cyber space legal and regulatory frameworks on online consumer protection in Kenya.

iv) To determine the effect of cyber security infrastructure on online consumer protection in Kenya.

3.3 Research questions

i) How does cyber security governance affect the online consumer protection in Kenya?

ii) What if the effect of Cyber security research and development on online consumer protection in Kenya?

iii) To what extent do cyber space legal and regulatory frameworks influence online consumer protection in Kenya?

iv) How does cyber security infrastructure affect online consumer protection in Kenya?

4. Scope of the Study

The study will analyze the influence of cyber security strategies on online consumers in Kenya using a descriptive study design. It will major of four independent variables including Cyber security governance, Cyber security research and development, Cyber space legal and regulatory frameworks and last cyber security infrastructure. The target population for this study will be drawn from two local online shops in Kenya (Jumia and OLX). The study population will include top management, middle level management and junior staffs. The session paper No. 2 of 1992 and the baseline survey of 1999 clusters Kenyan enterprises in the following categories; micro enterprises (1-9 employees), small enterprises (10-49 employees) and medium enterprises (49-99) employees. Large enterprise 100 employees and above RoK (1992) and with both Jumia Kenya and OLX Kenya falling under SMEs, a total of one hundred (198) will be considered for the study and the questionnaire will be used as the study instruments.

5. Limitation of the Study

There are some limitations that were experienced during this study. There were challenges in obtaining information from respondents due to the sensitivity of information. Some participants also chose not to answer the questionnaires due to commitment or fear of research intentions. To mitigate this, an introductory letter from the university was used to assure them of the research purpose and the fact that the findings would be used purely for academic purposes. Since questionnaire was used as an instrument for data collection, some respondents were reluctant in filling the questionnaire and some opted to return later or not return at all. In such instances the researcher left the questionnaires with the respondents and returned later to collect once they had been filled.

6. Empirical Review

6.1 Cyber security governance

Researchers in the past have had interest in cyber security strategies in several ways. Iginio and Nanjira (2015) did a research on cyber security and cyber resilience in East Africa, Magutu et al., (2011) studies effects of cyber-crime on state security: Types Impacts and mitigations with the fiber optics deployment in Kenya. TESPOK (2014) did a research on rethinking cyber security-An integrated approach: processes, Intelligence and Monitoring. Kimwele et al., (2005) also did a study on adoption of Information Technology security, case study on Kenyan medium and small scale enterprises. According to Suraiya, Nur and Zabil (2012) in the study on impact of consumer awareness and knowledge to consumer effective behavior in Malaysia employed survey technique to measure the three variables, consumer awareness, knowledge and behaviors and find out that there is a relationship between awareness and effective consumer behavior. It also found out that unawareness leads to ignorant and affects consumer’s ability in protecting and upholding their rights. The study also reveals that
consumer awareness differs based on locations, those in urban centers showed less awareness compared to non-urban dwellers.

Rainer and Tyler (2012), in the study on how consumers react to cybercrime found out that despite the huge benefits internet has brought to the society and efficiency it has brought to commerce, cybercrime has posed a threat to the benefits. Cybercrime has further created greater opportunity cost hence deterring online participation such as banking and shopping. This has been due to factors including experiencing cybercrime, being exposed to news about cybercrime and concerns about cyber-crime.

6.2 Cyber security research and development
According to Malala (2014) in her study on consumer protection for mobile payments in Kenya. An examination of fragmented legislation and complexities it presents for mobile payments found out that data protection has been a challenge to regulators who protect consumer rights to privacy and officials of law enforcement, combating money laundering. This is due to continuous innovations by fraudsters. Unauthorized access to customer’s information is on the rise as personal data transmitted via mobile phone are handled by agents and employees of financial institutions, customers equally can access the information remotely. Lack of customer education and exposure to new financial services has led to data security risks. The study further exposes the legislation gap as it does not define who is privy to mobile money trail and also the circumstances such orders may be obtained. This poses challenge to mobile operators on how to keep customer information safe and also to the regulators on how to safeguard their money from money laundering.

Developed nations like USA has got an informal organization of government managers who sponsor information security research within, named INFOSEC research council (IRC) Homeland Security (2009) IRC has got regular member representatives from many organizations including central intelligence agency, Air force, Army and Homeland security agency among others. IRC drafted Hard Problem list that covered desirable research areas based on the challenges experienced within USA according to IRC member missions and the Government observations. With the evolution of technology, IRC keeps on updating their list to cover new threats. In 2005 the hardest and most critical challenge in their list included insider threats, availability of Time-Critical system, information provenance, Security with privacy, situational understanding and attack attribution, building scalable secure systems and global scale identity management. Homeland Security (2009)

6.3 ICT Legal and Regulatory Frameworks
Researchers in the past have had interest in ICT Legal and Regulatory frameworks Kilonzno (2007) carried out study on electronic banking in Kenya, the study revealed that there are no specific laws governing electronic payments in Kenya and hence a legislative vacuum. The existing banking laws have reached the flexibility limits therefore amendments need to be made to address issues of electronic banking. The national ICT policy of 2006 needs to be revised to focus on network integrity, trust, security and e-commerce. The consumer protection Act no. 46 of 2012, which commenced working in December, 2013 talks about protection of consumer rights, protecting consumers from unfair practices and rights and obligations protecting consumer agreements but does not touch on online consumers.

In the Kenya information and communications act, section 84U states that no license under the act can deny customers access to the internet unless under payment breach or just terms, however the just terms has not been expressly defined Kenya Human Rights Commission(KHRC), (2014). Internet service providers can reduce and regulate internet speeds at will to its customers downloading large volumes of data as there is no legislation in place governing this. KHRC (2014). Section 30 and 31 of the Kenya communications act of 2009 protects customer privacy and interception of private messages through a licensed telecommunications system unless in the line of business by the telecommunications provider, however this provision is weak and prone to abuse whenever there information shared has not been disclosed. In addition there is little or no legislation in Kenya that protects customer’s information under the custody of third parties, that stipulates who can access the personal data, how it should be stored and what it can be used for (KHRC, 2014)

6.4 Cyber security Infrastructure
The cost of putting up an integrated cyber security infrastructure is relatively high Onufwoko (2009) studied factors influencing the use of ICT for learning among students at technical colleges in Nairobi focusing on time, ICT infrastructure, expertise and cost of using ICT and student to computer ratio in general. The GoK (2014) in the cyber security strategy report identified enhancing cyber security posture through protecting the critical information infrastructure as one of the pillars of vision 2030. The report further indicates the GoK is
promoting ICT usage through an undersea and terrestrial cable besides network installations, improved wireless technology and e-government services.

With the increase in ICT usage, Kenyan citizens have equally been exposed to cyber risks. Souter and Kerrets (2012) did a study on internet governance in Kenya—an assessment for the internet society, observed that the internet connectivity in Kenya has improved with the arrival of submarine cables along the east African coast. Kenya and its neighbors depended on satellite connection which is expensive and offer lower bandwidth. The two submarine cables along the Mombasa coastline are TEAMS (The Eastern Africa Marine System), Seacom, EASSy (The Eastern Africa Submarine System) and LION2 connecting Mombasa and the island states of South AFRICA. The presence of four submarine cables has greatly led to increased bandwidth availability.

6.5 Online Consumer Protection

Njuguna et al., (2014) did a study on consumer awareness and its effects on consumerism in Kenya; a survey was conducted on household consumers in Nakuru County. The study found out that most consumers are aware of their rights though majority of the consumers were not using the established consumers rights protection mechanisms. The study recommended a policy on consumer education and manufactures to set a division for dispute resolution. Malala (2013) did a study on consumer protection for mobile payments in Kenya. An examination of fragmented legislation and complexities it presents for mobile payments. The study found out that there is no proper legislation for mobile payments in Kenya as the mobile payments is a new entrant into the market. This has eventually left the regulatory environment vulnerable to various risks which may end up affecting consumers.

According to Misiani, Makanu and Kuria (2014) in the study of Security, privacy and trust issues surrounding e-commerce in Kenya, there has been an upward growth in e-commerce services and business and as a result, there is need for improving the perception of consumers on the safety on online transactions and the safety of their financial details from unauthorized access as previous studies have pinpointed security as the major ethical factor in the online context. Online consumers need protection against fraudulent and unfair business practices and whenever aggrieved, they should be able to gain redress. Companies equally need to improve on data integrity, confidentiality and authenticity of data by adopting a set of industry standards to protect consumer privacy to backup the formal legal obligations. E-commerce businesses can as well build consumer trust through industry best practice (Misiani, Makanu and Kuria, 2014)

6.6 Research gaps

Online consumer protection is still not well addressed in developing nations like Kenya. Most recent studies have majored on existence of e contracts and their validity in Kenyan laws Magalla (2013) however there is no existing study that has addressed the awareness of online consumers on electronic contracts. Online consumer awareness on their rights has also not been properly captured in the previous studies, according to Mwaura, Oyugi and Oyugi (2014) in their study on consumer awareness and its effects on consumerism in Kenya: a survey conducted on household consumers in Nakuru county found out that most consumers are aware of their rights though few use the provided mechanisms to address their grievances, no previous study has gone deep to find out the exiting online consumer protection mechanisms in Kenya and the level of awareness by consumers on the same. According to Kilonzo (2007) in the study on challenges posed by electronic banking in Kenya there are legal gaps on data protection, cyber security and information sharing laws. None or little has also been captured in the previous studies on the participation of online consumers in dispute resolution. (CBK, 2015)

7. Methodology

7.1 Research design

A research design refers to a plan or a map or a framework that acts as a guide to a researcher on how to execute the investigation. Kothari (2004) defines a research design as the scheme, outline or plan that is used to generate answers to research problems. The study adopted a descriptive research design which is appropriate where the study seeks to describe the characteristics of certain groups, estimate the proportion of people who have certain characteristics and make predictions. Descriptive research design was adopted due to its ability to reduce the bias and maximizes the reliability of evidence collected. (Mugenda & Mugenda, 2008)

7.2 Sample size and sampling procedure

Researchers may select a sample due to various limitations that may not allow researching the whole population. According to Kothari (2004), a representative sample is one which is at least 10% of the population. Therefore a sample of 100 respondents which is considered a representative was arrived at using slovin’s formula.
Using slovin’s formula: \( n = \frac{N}{1 + Ne^2} \).

Where;
\( n \) = sample size
\( N \) = total population i.e. 198 employees
\( e \) = Error tolerance. The study confidence level will be 93% which will give a margin error of 0.07

The sample size is calculated as follows;
\[
\begin{align*}
N &= 198 \\
e^2 &= 0.03^2 \\
\frac{N}{1 + Ne^2} &= \frac{198}{1 + 198 \times 0.03^2} \\
n &= \frac{198}{1.9702} \\
n &= 100
\end{align*}
\]

The sample size was 100 employees.

Stratified random sampling method was used to select respondents from each subgroup, and then simple random sampling method using proportionate stratified sampling formula \( n_1 = \frac{n}{N} \times N_1 \) to select respondents sample from various strata.

Where:
- Top Management = \( \frac{100}{198} \times 20 = 10 \) employees
- Middle Management = \( \frac{100}{198} \times 40 = 20 \) employees
- Low Level = \( \frac{100}{198} \times 138 = 70 \) employees

Table 1: Sample size distribution

<table>
<thead>
<tr>
<th>Category</th>
<th>Population</th>
<th>Sample Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Management</td>
<td>20</td>
<td>10</td>
</tr>
<tr>
<td>Middle level</td>
<td>40</td>
<td>20</td>
</tr>
<tr>
<td>Low Level</td>
<td>138</td>
<td>70</td>
</tr>
<tr>
<td>Total</td>
<td>198</td>
<td>100</td>
</tr>
</tbody>
</table>

The sample size involved ten top managers, twenty middle level managers and seventy low level managers. The numbers were shared equally between Jumia Kenya and OLX Kenya.

7.3 Data Collection Instruments

The first objective of data collection was to conduct a pilot testing to establish the accuracy and appropriateness of the research design and instrumentation and therefore improve on its usage. Secondly, to fine tune the questionnaire so that respondents in the major study would not have any problem in answering the questions. The respondents were conveniently selected since statistical conditions were not necessary in the pilot study (Kothari, 2004). The questionnaire was hand delivered and administered at the respondents’ place of work to ensure objective response and reduce non-response rate. The results of the pilot study were included in the main study to follow immediately after the pilot testing.

8. Findings, Data Analysis and Discussion

8.1 Response Rate

The study targeted a total of 100 respondents. However, while 83 respondents completed and returned their questionnaires, 17 respondents did not return their questionnaires. This translates to a response rate of 83%. The response rate of 83% is considered satisfactory to make conclusions for the study. According to Mugenda and Mugenda, (2003) a response rate of 50% is adequate, 60% is good and above, while 70% is rated very good. Bailey (2000) also asserts that a response rate of 70% is very good while 50% response is adequate.

The high response rate was as a result of the data collection procedures used; the researcher self-administered questionnaires to the respondent’s place of work then did a follow up to fine tune the questionnaires to ensure better understanding. Where the respondents were busy, the researcher left the questionnaires behind and collected later after being duly filled. This was also done after pre notification of the participants.

8.2 Reliability of the Results

To measure the reliability of the data collection instruments an internal consistency technique Cronbach’s alpha was computed using SPSS. The reliability was computed from the data collected in the pilot study. The data obtained from these respondents was analyzed using SPSS Cronbach’s
Table 2: Reliability Results

<table>
<thead>
<tr>
<th>Constructs</th>
<th>Cronbach's Alpha Values</th>
<th>No of Items</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT legal and regulatory framework</td>
<td>0.70</td>
<td>17</td>
<td>Accepted</td>
</tr>
<tr>
<td>Cyber security governance</td>
<td>0.971</td>
<td>6</td>
<td>Accepted</td>
</tr>
<tr>
<td>Cyber security infrastructure</td>
<td>0.960</td>
<td>9</td>
<td>Accepted</td>
</tr>
<tr>
<td>Cyber security research and development</td>
<td>0.956</td>
<td>9</td>
<td>Accepted</td>
</tr>
<tr>
<td>Online consumer protection</td>
<td>0.728</td>
<td>4</td>
<td>Accepted</td>
</tr>
</tbody>
</table>

Table 2 indicates that the obtained data was reliable since data obtained from all independent variables had a Cronbach’s alpa values of between 0.7 to 0.960 and this was above 0.7 satisfying the threshold required that an alpha coefficient higher than 0.70 indicates that the gathered data had relatively high internal consistency and could be generalized to reflect opinions of all respondents in the target population on influence of cyber security strategies on online consumer protection in Kenya.

8.3 Regression Analysis

Through regression analysis, the Coefficient of determination (R square) was used to show the extent to which any change in dependent variable was explained by the independent variables on online consumer protection in Kenya, collectively. Table 3 illustrates the value R square.

Table 3: Coefficient of determination on online consumer protection

<table>
<thead>
<tr>
<th>Model Summary</th>
<th>R Square</th>
<th>Adjusted R Square</th>
<th>Std. Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.909</td>
<td>0.826</td>
<td>0.199</td>
</tr>
</tbody>
</table>

Findings indicated that ICT legal and regulatory framework, cyber security governance, Cyber security infrastructure and Cyber security research and development collectively influence online consumer protection by 82.6% as indicated by the coefficient of determination (R square). This is also an indication that other factors (except ICT legal and regulatory framework, cyber security governance, Cyber security infrastructure and Cyber security research and development) explain 17.4% of any change in online consumer protection in Kenya.

8.4 Analysis of Variance (ANOVA)

ANOVA shows relationship in the variables between and within the measure of the dependent variable. It reflects the magnitude the model has on the data compared to those that are not considered in the model (residual).

Table 4: Analysis of Variance (ANOVA)

<table>
<thead>
<tr>
<th>Sum of Squares</th>
<th>df</th>
<th>Mean Square</th>
<th>F</th>
<th>Si g.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regression</td>
<td>20.256</td>
<td>4</td>
<td>5.064</td>
<td>12</td>
</tr>
<tr>
<td>Residual</td>
<td>4.275</td>
<td>78</td>
<td>0.040</td>
<td>28</td>
</tr>
<tr>
<td>Total</td>
<td>24.531</td>
<td>82</td>
<td>0.040</td>
<td></td>
</tr>
</tbody>
</table>

Predictors: (Constant), Change in ICT legal and regulatory framework, cyber security governance, Cyber security infrastructure and Cyber security research and development

Dependent Variable: Online consumer protection

According to the ANOVA results, the probability value for the regression model was 127.928. Given that FCritical (2.447) is less than FCalculated (127.928) then the criteria for decision making is to reject the null and instead accept the alternative hypothesis and conclude that the four independent variables (ICT legal and regulatory framework, cyber security governance, cyber security infrastructure and cyber security research and development) are critical in determining online consumer protection in Kenya.

9. Summary of the Findings

From the findings, all the respondents agreed that cyber security governance influence online consumer protection. The average effect of cyber security governance on online consumer protection was rated at 4.5 out of 5 with a deviation of 1.0. The effect on cyber security threats was rated at a mean of 4.8 and standard deviation (Sdv) of 0.9. Cyber security awareness is second (mean = 4.7; Sdv = 0.7). Respondents further highlighted the various ways in which online consumer protection is affected by safe information sharing. The positive influence was
asserted to be: improved consumer confidence; safe online transactions and enhanced online business. However, there were some respondents who expressed that information sharing has a negative effect. Their concern was that, often, the safe information given by the client to user of that information ends up being shared to marketers without knowledge of the provider of the information. This in turn makes some customers vulnerable to cyber fraud.

The extent of the influence by various determinants of cyber security research and development on online consumer protection was rated at 4.4. Pertaining to this aspect, the rating for the role of private sector and industry was a mean of 4.5 each. The scores for the role of government and academia were 4.3 and 4.2 respectively. There was a strong assertion that cyber security research and development affect online consumer protection with a vast majority (89.2%) of the respondents affirming this. Most of the respondents posited that it helps to identify the gap in cyber insecurity counter measures and its influence on online consumer protection. There were also assertions that it helps customers to be protected against malicious data theft through improvement on cyber security weakness. Cyber security space was asserted to have a great influence on e-consumer protection with a mean of 4.2. In this regard, its effects on insider threats and insecure web applications/platforms were rated the highest with a mean of 4.5 and 4.4 respectively.

Findings indicated that the effect ICT legal and regulatory frameworks on online consumer protection occurs through the setting of the basic ICT security policy that ensures online customers are not exposed to online security threats. Others alleged that it makes customers aware of online fraud. Other effects mentioned include lengthy process in online transaction, stimulation of innovation and creating of a level playground. The extent of the influence of ICT legal and regulatory frameworks was rated at 4.4 with a low deviation of 0.7. Regarding this aspect, the mean ratings for the effect of data protection laws, cyber security laws and regulations compliance were 4.5, 4.5 and 4.1 respectively. There were only 39.8% of respondents familiar with consumer protection policy. An overwhelming majority of them (91.6%) affirmed that the procedures on regulation of online transactions are inaccessible to the consumers.

It was further revealed that 48.2% were knowledgeable about electronic contacts to a very low extent while 24.1% were moderately informed, with only 15.6% alleging to be greatly informed. Regarding Consumer Protection Acts in Kenya that addresses internet agreements, findings indicated that most of the respondents (60.2%) were not aware of these Acts. Findings also indicated that 77.1% of the respondents were lowly informed on the cancellation of internet agreement procedure as per clause 34 of the Consumer Protection Act of Kenya.

The overall effect of cyber security infrastructure on online consumer protection was rated at a mean of 4.3. On this aspect, the effect of cost of ICT was rated at a mean of 4.6 while the effect of cyber security standards was rated at 4.1. It was strongly affirmed that proper and adequate cyber security infrastructure like firewalls can greatly help improve on consumer data. Moreover, cyber security infrastructure was purported to enhance accessibility to online ecommerce compatible devices. Even so, some respondents pointed out that lack of elaborate cyber security infrastructure has lead to poor online consumer protection. ICT infrastructure was accused by some as having lead to an increase in cyber attacks.

The effect exerted on online consumer protection was assessed with reference to three major aspects including: customer redress, dispute resolution and improved data sharing. The overall effect was rated at a mean score of 4.5 with a deviation of 0.8. The effect exerted on improved data sharing, customer redress and dispute resolution was rated at a mean of 4.7, 4.4 and 4.4 respectively. Regarding online customer redress mechanism in place, majority of the respondents (80.7%) were unaware of such mechanisms. There were several (38.6%) respondents who attested the existence of dispute resolution division while 19.3% denied. In shops where there are no dispute resolution divisions, respondents expressed that disputes from unsatisfied customers are handled through avenues such as court proceedings, customer care-calls and feedback from customers followed by recall and replacement of products or offering the service again.

10. Conclusions

In the light of the findings from this study, it can be inferred that cyber security governance has a strong influence on consumer protection in online business transactions. Good governance of cyber security comes up with good policies that influence customer protection. This is mainly through the proposition and implementation of measures to protect the transmission and exchange of data on the internet. Even so, it sometimes becomes a challenge to enforce of such regulations, either because the enforcement mechanism is weak or the enforcers themselves are reluctant to enforce. On the same note, safe information sharing can have both positive and negative influence. The positive influence is through improved consumer confidence; safe online
transactions and thus enhanced online business. On the other hand, the negative effect occurs by virtue that, the safe information that may be shared by the client to user of that information sometimes end up being shared to marketers without knowledge of the provider of the information. This in turn makes some customers vulnerable to cyber fraud and may also affect the integrity of the organization.

This study also concludes that cyber security research and development has a great influence on online consumer protection. In this regard, the role played by the private sector and the industry as well, has the greatest effect on online consumer protection. Generally, cyber security research and development helps to identify the gap in cyber insecurity counter measures and its influence on online consumer protection. It further helps maintain the pace and complexity in development of cyber threat and it is often futuristic. In this way, it helps pre-empt on eminent cyber danger, thus devising means of possible elimination or reductions of the real and imagined threat. This is achieved through improvement on cyber security weakness observed. Still on this note, cyber security space strongly influences e-consumer protection. Its greatest effect is on insider threats and insecure web applications/platforms, with minimal effect on online advertising compliance.

The effect of ICT legal and regulatory frameworks on online consumer protection is also great. With regard to this, data protection laws and cyber security laws exerts the greatest influence. Generally, the effect exerted by ICT legal and regulatory frameworks is mainly through the setting of the basic ICT security policy that ensures online customers are not exposed to online security threats. Even so, it could prolong the process of online transaction. Moreover, though it seeks to improve online consumer protection, weak legal frameworks in Kenya have to an extent contributed to poor online consumer protection. Most of online shops are inadequately informed about the consumer protection policy. This could be due to high inaccessibility of the procedures on regulation of online transactions. Not only are they not well familiar with electronic contacts, but also they are less informed about Consumer Protection Acts in Kenya that addresses internet agreements. In addition, very few are familiar with the cancellation of internet agreement procedure as per clause 34 of the Consumer Protection Act of Kenya.

From the findings, it can also be inferred that cyber security infrastructure greatly determines online consumer protection. In this regard, the most determinant factor is the cost of ICT. Proper and adequate cyber security infrastructure like firewalls can greatly help improve on consumer data. It further provides the basic ICT security protection for customers’ privacy during online transactions. As such, customers are protected against fraud; blocking unwanted sites and enforcing processes and procedures. In Kenya however, lack of elaborate cyber security infrastructure has to some extent lead to poor online consumer protection, consequently increasing cyber-attacks. Overall, it can be concluded that cyber security strategies exert quite a great effect on online consumer protection. Although the most affected aspect is improved data sharing, customer redress and dispute resolution are also significantly affected.

11. Recommendations

Considering the findings of this study, the following recommendations are proposed:

The government should ensure that, in as much as regulations geared towards online consumer protection are developed, enforcement mechanisms are strengthened to ensure that the regulations are fully enforced. Otherwise, if regulations are well constructed, without appropriate enforcement, their positive contribution will be minimal. The e-business structure should be designed such that, any information cannot be shared to the marketers without knowledge of the provider of the information. This could help to ensure that customers are not subjected to cyber fraud.

There is also need to strengthen the legal frameworks in the country to ensure adequate online consumer protection. However, this should be carefully done to see to it that ICT legal and regulatory framework does not prolong unnecessarily, the whole process of online transaction which is otherwise expected to be fast. It is also important that awareness be improved amongst online shops about consumer protection policy. This could be achieved through improving the accessibility of the procedures on regulation of online transactions.

The online shops should also familiarize themselves with electronic contacts and Consumer Protection Acts that addresses internet agreements in the country. Cyber security infrastructure also needs improvement. This could be realized through the proper use of firewalls and other ICT security measures to ensure adequate online consumer protection. This could go a long way in reducing incidences of cyber-attacks which in turn could boost consumers’ confidence in online businesses.
12. References


[10]. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests


