Enhancing Data Breach Risk Management: A Case Study of Kenyan Commercial Banks

Silas Nzuva.

[#]*School of Computing and Information Technology*
Jomo Kenyatta University of Agriculture and Technology
Nairobi, Kenya.

Abstract *— With the recent technological advancements, there is the need for a business organisation to employ risk management strategies that are aimed at combatting the incessant data breaches, whose negative implications are many. The main aim of the study is to investigate the current information security risk management strategies employed by the Kenyan Banks and suggest measures that the banks can adopt to bolster them and ameliorate adverse effects on their financial performance that is associated with a data breach. The research was carried out using quantitative descriptive design. Data was collected from 20 Kenyan banks, which were selected randomly from the 44 banks operating in the Kenyan financial sector. The design of the questionnaire design was informed by the general deterrence theory as well as the information systems security theory. The results of the study were then analysed using Microsoft Excel and Statistical Package for Social Sciences (SPSS). The results of the study indicated that the Kenyan Commercial banks have average risk avoidance measures, are reluctant to transfer their risks to third parties through outsourcing, and lack robust risk mitigation measures, specifically business continuity plan and disaster recovery plans.*

Keywords *— data breach, cyber attacks, data protection, data confidentiality, data protection strategies, risk management strategies.*

I. INTRODUCTION

A breach of organisational information resources has become a significant concern for business organisations. With the recent technological advancements, there is the need for a business organisation to employ risk management strategies that are aimed at combatting the incessant data breaches, whose negative implications are many. A breach of information systems security is an activity that occurs within the organisation network and which often results in access to unauthorised data [2]. Such a breach can lead to loss of data, deletion of substantial information, manipulation of the stored data, and also theft of such data [44]. According to the Kenyan Data Protection Bill of 2018 and Article 31 of the Kenyan Constitution , it is the duty of an organisation to ensure that its information resources are secure and cases of data breaches are mitigated [47],[48].

One of the indicators of how an organisation is faring is its financial performance [21]. The financial performance of an organisation is measured by the use of different tools, including but not limited to financial statements and cash flows. When evaluating the financial performance of an organisation, it is always important to consider how the operational costs of the organisation are in line with the revenues from the sales [21]. If the operational costs of an organisation are higher than its revenues, then the organization is making losses and consequently can be considered to be financially underperforming.

An individual infiltrates the information systems of an organisation for various reasons. One of the most common reasons why information systems in an organisation are breached is to steal or compromise the customers` data [37]. Martin et al. add that many of the security breaches reported are due to the presence of specific information of customers, which can be used for fraudulent purposes, specifically in the banking sector [23]. The implications of a data breach are many, including but not limited to increased customers' litigation, tainted brand image, and reduced performance of the firm in both short term and long term [37].

A security breach can have a negative impact on the market value of an organisation. Research by Soomro et al. estimated the impact that security breaches had on cumulative abnormal return (CAR) while considering the type of security breach [37]. Security breaches have an adverse impact on CAR without even considering the type of security breach. The researchers also found out that any security breach, regardless of its nature was received negatively by investors, especially in publicly traded firms. Firms that have experienced security breaches lose up to 2.1% of their stock market value within the first two days after the announcement of the breach within the organisation. [37]

The risk management strategies adopted by an organization determine the aptness of the organization in responding to data breaches. Risk management strategies in an information system setting cover three main facets, which include risk avoidance risk transference and risk mitigation [36]. It is, therefore, the responsibility of a firm to ensure

that each of these three facets of risk management is well developed and construed in a manner that ensures optimal responsiveness to data threats.

A. Research Problem

Information systems can have a recurring adverse effect on the performance of the Kenyan commercial banks. This is because, despite the one-time costs that emanate from the breach, the organisation also suffers gradual residual losses regarding the lost grip on the customers as well as the tainted customer perspectives regarding the [35]. Therefore, there is the need to carry out research to establish the effectiveness of the various risk mitigation strategies in preventing and/or responding to data breaches to ensure minimal negative effect on the financial performance of the firm. A breach of information systems often may indicate poor compliance with best practices in the industry, and indicates poor compliance with the Kenyan government regulations regarding the protection of third party data held by business organisations as per the Kenyan Data Protection Bill of 2018 and Article 31 of the Kenyan Constitution [47], [48].

II. LITERATURE REVIEW

The increased need for resilient information systems has resulted in vast technological advancement. Dwivedi et al. carried out an investigation to elicit the success and failure rates of information systems and found out that though some information systems fulfil the purpose for which they were developed, a larger number usually fails due to the complexity of the system [17]. Using a quantitative study that utilised survey questionnaires from information systems professionals, the researchers established the need for new strategies and approaches in information systems research in order to provide sufficient guidance and insights that would guide the managers in ensuring adoption of optimal IS strategy in order to reduce the failure rates [17]. The researchers explain that a failure in the information system can emanate from both within the organisation or from an external source. In line with this, it is the responsibility of the organisational managers to ensure that the information resources are protected against accidental or deliberate access to data, either by the organisational personnel or external perpetrators. The researchers recommended the need to get a clear picture of the Information Technology essence in an organisation and cessation of perceiving IT as a standalone artefact [17].

The study by Soomro et al. indicates the need for a more holistic approach to information security management [37]. Through a systematic review that enlisted 39 studies, the researchers denoted that the management of an organisation plays a critical role in ensuring the security of the organisational information. According to Soomro et al., organisations that exhibit promiscuous policies such as weak acceptable use policy are more prone to information insecurity as compared to the organisations that utilise strict policies [37]. On the same point of view, the researchers also established that managerial activities and specifically, development and implementation of data protection policies, human resources management, IT and business alignment, IT infrastructure management and the effectiveness of the information system architecture bears a significant impact on the ability of an organisation to warrant security of the stored data. In their suggestion for a holistic approach, Soomro et al. emphasise that the managers should steer information security by ensuring that the workforce and all the organisation resources are construed in a manner that promotes the achievement of the corporate objectives [37]. Further, Soomro et al. also insist on the need for having a strong risk management strategy that is aimed at reducing and possibly eliminating the impact of unwarranted risks [37].

The research by Safa outlines the various concepts and aspects that must be addressed or an organisation to comply with the various information security standards [34]. Compliance with the various national and international standards on information systems security bears the ability to protect the information assets of an organisation [34]. Personal norms, commitment, and attachment were as well found to be correlated with information security [34]. In an organizational setting, the management of usually exhibits significant control over the majority of these variables

It is impossible for a business organisation to operate today without relying on the various technologies that have been developed to simplify and improve productivity and performance in an organisation. The emergence of industry 4.0 has been instrumental in steering business organisations to adopt better automation and technologies that are geared towards improved efficiency and performance [33]. In line with this, Prajogo et al. argue that today business organisations are operating within a network of cyber-physical systems and the internet of things, and hence in order to remain relevant and productive, a firm has to adopt such technologies and sync them with its overall business model [31]. However, despite the benefits that are associated with the adoption of robust and resilient technologies, various downsides have also been noted. Just as the technology has evolved, so has the cybersecurity threats, as well as the skills possessed by the attackers.

Unlike decades before, modern-day cyber attackers use sophisticated systems and software to propagate attacks on organisation networks. Combating such threats has become a major function often the Information Technology department, and over the years has seen the role of information systems security professionals become more apparent

and relevant. The security breaches in organisational information systems are diverse, an include but not limited to the deployment of viruses and worms, web defacement, sabotage of information resources, denial of services, and theft of propriety information [12]. Over the last couple of years there has been a sharp increase in the number of security breaches reported by organisations despite the organisation being aware of information security importance [33]. A study conducted by Prajogo et al. shows that the majority of the data breach cases usually go unreported, due to the fear that if such reports are exposed to the public, the organisation may directly, or directly suffer from the tainted brand image as well as the loss of customer trust [31]. Cavusoglu et al. note that the costs of a security breach on organisation information systems are hard to quantify, and, in many cases, the costs are usually poorly quantified [12].

III. THEORETICAL FOUNDATIONS

A. The General Deterrence Theory (STS)

While various theories have been developed with respect to the protection of organisational information resources and data breach risk management, the general deterrence theory stands out as one of the most intriguing theories, which is likewise applicable in the present study. According to Wortley and Sidebottom, the theory focuses more on sanctions and disincentives against actions that compromise information security; hence, it is considered as a risk avoidance theory [42]. The theory takes into consideration two main variables; risk avoidance and risk mitigation. A possible breach in an organization's information system can be addressed either of the four phases of preventing information systems breach, which includes deterrence, prevention, detection and remedy [1].

According to the theory, the measures and actions taken by the management are capable of deterring information security lapse by preventing abuse, misuse of the information resources, or committal or participation in illegal dealings. Essentially, this theory holds it that it is the responsibility of the organisational management to ensure strong policies and measures are put in place to determine the potential data breaches as such the theory proposes a proactive approach to information security, rather than a reactive approach [26].

Deterrence (Risk avoidance strategy): According to the theory, any deliberate breach of an organisation system commences from a contemplated abuse. However, there should be sufficient disincentives, polices, and physical security to deter any malicious activity perpetrated by individuals within or outside the organization [1]. The individual at this stage may decide to attempt the abuse or withdraw from attempting the abuse. At this phase, no harm to the organisation information is done.

Prevention (Risk avoidance strategy): This step entails invoking preventive measures to ensure that the perpetrator does not compromise critical data. The perpetrator can then proceed to attempt the abuse; in this case, the abuse can either be successful or unsuccessful. However, there should be sufficient physical obstacles, authentication, protocols, and procedures to prevent any unauthorised cases to the organization's information [1]. Successful abuse implies that the perpetrator has managed to penetrate the information system security measures by levering on the existing vulnerabilities or create new loopholes. At this level, the organisation information system is already at very high risk as the decision to misuse destroy, steal or manipulate the data lies in the hands of the perpetrator.

Detection (Risk mitigation): At this phase, the breach has already occurred, and further security of the organizational information lies on the ability of the intrusion detection systems to notify the necessary security personnel of the detected breach.

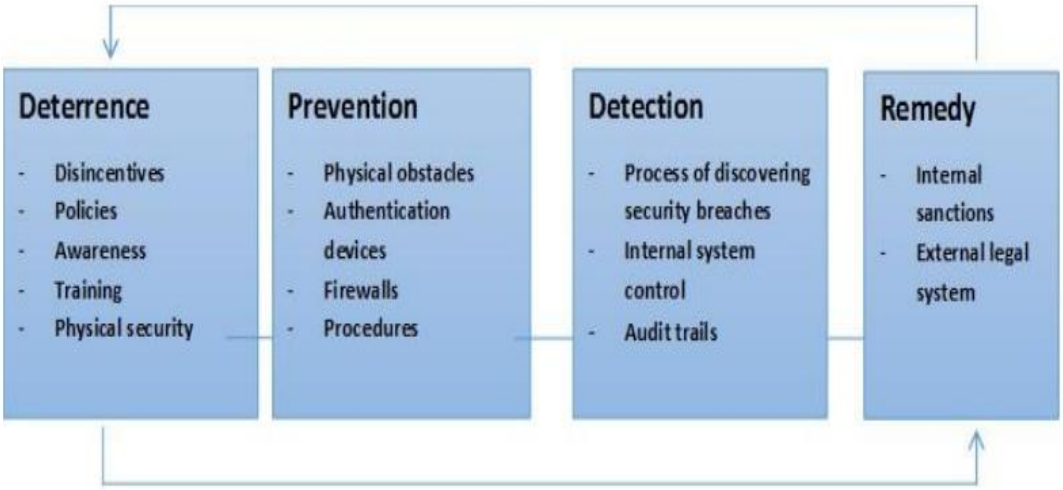

Fig. 1: A theoretical model derived from the general deterrence theory (Source: Alanezi & Brooks, 2014, p. 3)

However, the existing intrusion detection mechanism, internal system controls, and audit trails may or may not be able to detect the breach in time, depending on their accuracy and reactiveness in identifying data breaches [1]. After a successful abuse, if there lacks a proper mechanism to deal with intrusion detection and initiate the necessary measures, the perpetrator then escalates the breach to undetected misuse.

Remedy (Risk Mitigation): At this stage, a successful breach has occurred, and it is the responsibility of the management and the IT personnel to implement the appropriate measures as defined in the risk management strategies in order to ensure reduced adverse effects on the organization's operations, brand image, and overall performance. The adversity of the breach at this point relies on the ability of the existing risk mitigation measures to resolve the issue in time and ensure minimal damage.

The general deterrence theory is well suited in strengthening the security policies of an organisation and assessing and evaluating the effectiveness and efficiency of the policies relative to the information security, as well as the risks surrounding the information system [42]. Nevertheless, Alanezi and Brooks recommend the synchronisation of the general deterrence theory with the Situational Crime Prevention and the Rational Choice Theory on devising appropriate organisational strategies to combat data security threats [1]. Together these theories are not only capable of steering proactive approach to data security but also ensuring that the reactive approaches employed are rational and optimal and positively contribute towards the achievement of the corporate objectives [13].

B. Information System Security Theory (STS)

The modern security events are not attributed to a failure in a single level of control or technological mechanism but due to a myriad of failures [45]. The authors are calling modern information system security challenges as mixed and blended attacks. They note that bypassing one level of security control is easy, and once inside, the attacker can change tact and gain more access to the information [45]. Based on this set of information, Conklin and Dietrich argue that modern information security threats can only be handled through the use of complex and integrated systems [45]. A system involves a collection of entities that act in tandem with the objective of achieving a certain purpose. Entry to a system may be both at the input and at the output when the system is providing information back at the environment. Therefore, a simple system only regulates information breach from either the input or the output or from both sides. Conklin and Dietrich define this system as weak and extremely vulnerable to security breach especially in the era of advanced technologies [45].

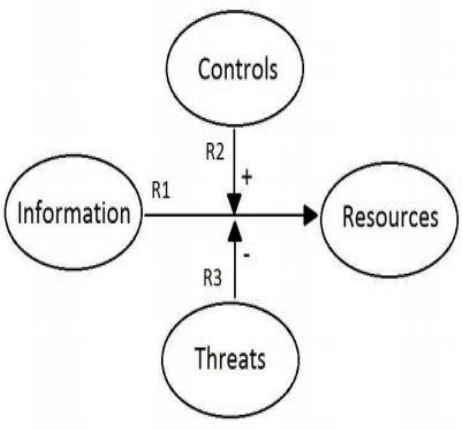

Fig. 2: A model representation of the information system security theory (Sources: Horne, Ahmad & Maynard, 2016, p.5)

As a result, Horne, Ahmad, and Maynard evaluate a system theory model that propagates for complex systems for information system infrastructure [19]. This theory argues that a complex system as a whole has properties that are not directly attributed to individual system elements and they are referred to as emergent properties. The main argument is that security is an emergent property of a system that is not embedded in a single component but can arise from various levels or components [19]. System theory, therefore, posits the need for a complex system that has the capacity to protect the information system from various components or levels. This theory realises that information security changes with the nature of the environment and the issues of emergent and unknown states [19]. Hackers and cyber attackers are regularly developing malware, and other security bypasses that an information system may not have predicted. The information system security theory, therefore, takes into consideration the three variables of risk management; risk avoidance, risk transference, and risk mitigation [45].

A complex system will have the capacity to block or prevent such an attack of an unknown state as compared to a simple system that will be compromised. Second, there is an element of interdependence, as highlighted in the system theory. Systems theory propagates for engineering, designing, and developing multiple interconnected components in such a way that they function efficiently together to perform specific tasks that meet the specific needs of an organisation [19]. A single system may not be efficient or may lack the capacity to handle all the information system security needs. An integrated system has the capacity and is in a position to handle such cases efficiently [19].

One of the principles of system theory is that the depth of defence [45]. There should be a security guarantee and the capacity to achieve multiple and higher levels of protection. On the contrary, systems

theory model faces a challenge, especially in the social and human factors. It is evident that system theory propagates for complex systems. This implies that the operation of such systems is quite complicated, and it does not integrate social factors. There is a possibility of users feeling alienated when implementing system theory and ultimately fails to attain maximum effects of the information system [19]. This also brings the element of cost, time, and other resources. A complex system is costly and requires huge investments. Moderate and small firms that intend to embrace this theory might be disadvantaged, or they may fail to achieve their objectives from this theory of information systems [45]

IV. METHODS

A. Research Design

The study utilised a quantitative descriptive approach to describe the research without necessarily intervening using any form of treatment. A quantitative allows the researcher to capture a picture of the research population, which in this case, is the Kenyan commercial banks, through a sample that depicts the true characteristics of the population. The descriptive approach enabled the researcher to tell what it is, as opposed to inferential approach, which determines the cause and effect of a study. The descriptive approach allowed for the identification of attributes found in the phenomenon, thus, enabling the researcher to perform statistical data analysis for the entire population sharing such attributes.

B. Questionnaire Design and Administration

The researcher used a survey questionnaire as the main data collection tool. To ensure the validity of the research, the design of the questionnaire was informed by existing literature on data breach risk management strategies employed by the Kenyan commercial firms and the possible measures to bolster them and ameliorate adverse effects on their financial performance [39].

The questionnaire comprised of 10 questions with sub-questions, covering the four variables, and the demographic information. In designing the questionnaire, a 5-point Likert scale was the main measurement scale for the participants' responses. All the questions were closed-ended; this implied that the data obtained is pre-coded, and hence can be statistically analysed to give descriptive statistics that aided in answering the research questions presented. The pre-coded data using the Likert scale is also in line with the quantitative descriptive research design used in the study, and which is made to answer the "what" questions.

The survey questionnaire was designed following the two theories analysed in the theoretical framework with respect to risk management and was administered electronically using web links to the sampled participants. Specifically, the researcher used SurveyMonkey, an online platform for the administration and collection of electronic survey questionnaires. The participants accessed the survey questionnaires through a web link that was sent to them via electronic mail and messaging applications. The entire questionnaire was configured in a manner that each question "required an answer" before submission.

C. Research Population and Sample)

The research population in this study comprised of the banks operating in the Kenyan financial industry. According to the Central Bank of Kenya, by 31st Dec 2018, there were 44 licenced commercial banks operating in Kenya; these form the research population [49].

The sampling technique employed bears the ability to positively or negatively affecting the results of the study [10]. In the present study, the researcher employed the use of random sampling technique. 36 banks were then selected randomly from the 44 banks operating in Kenya (research population) operating in Kenya.

The researcher decided to engage two participants from each bank due to time and financial resource constraints. For one to be enlisted in the study, they had to meet the selection criteria: be holding a supervisory or managerial position in the IT department. Two participants were then selected randomly from the managers and supervisors within the IT department and contacted to participate in the study. As such, the researcher distributed a total of 72 questionnaires to individuals holding managerial positions relevant to Information Technology positions in their respective banks; this was the main inclusion/exclusion criteria used in participant selection.

D. Ethical Considerations

Consideration of ethical principles was addressed by ensuring that the participants' rights were respected and protected as well. This was achieved by ensuring that their participation in the study was voluntary, the details on the essence and use of the study were explicitly explained to them, and finally, the anonymity of their participation in the study was assured. First, the participants were supplied with the information sheet indicating the purpose of the study, its significance, how the results of the study will be used, and their required input to make the study a success. Secondly, the participants were required to sign a research participant consent form. For any of the participants to be allowed to participate in the study, they were to confirm having read and understood the information sheet supplied to them with respect to the present study. They were to also confirm that they had been given an opportunity to ask any questions relevant to the research through any appropriate communication channel. Further, the participants were to agree on taking part in the

questionnaire and that their participation was to be voluntary; they had the liberty to withdraw it without any prior notice or reason. Finally, the participants were allowed to append their signatures as a way to confirm their agreement to partake in the study. The research participant consent form contained the details of the researcher, signature, data, name of the researcher and the researcher's email. These details provided easy contact information in case the participants wanted to make any follow-up questions

The issues of anonymity and confidentiality were also parts of ethical considerations and were ensured in the study. The former involved making the identities of participants' unknown while the latter involved protecting the information offered by the participants. To guarantee anonymity, the participants were asked or allowed to provide personally identifiable information, such as names, addresses, and contact information. This made it impossible for the researcher to link specific questionnaire responses to a specific participant. Confidentiality was achieved by making sure that any personal information obtained from the participants is not exposed to the public

V. RESULTS

The questionnaires were distributed to 72, only 46 responded. This gives a 63.89% response rate, with the actual sample size being 46 (n=46). This implies that 26 (36.11%) participants did not participate in the survey. It is critical to note that none of the participants who did not turn out gave out the reason for not participating; hence, a future study is required to establish the observed lack of interest by the targeted group on the survey related to data security of their banking institution. The main aim of the study was to research the effectiveness of the existing risk mitigation strategies by banking institutions in Kenya in preventing and/or responding to data breaches to ensure minimal negative effect on the financial performance of the firms. The responses were collected in an electronic format.

The first question of the study related to demographics. The participants were asked to select their age group. As presented in **Error! Reference source not found.**, it is clear that the individuals aged 45-54 formed the largest percentage, followed by those with 35-44 years. Realistically, these age groups are characterised by high maturity since the majority of the individuals are mid-way in their professional careers.

The participants were once again asked about their highest educational qualification. According to the National Research Council, education is often used as a measure of knowledge, and hence the more an individual is educated, the more they are expected to be knowledgeable [27].

With respect to the protection of the banking information system, it is expected that banks should hire individuals who are highly educated and capable of ensuring that the information systems are in line with the organisational goals and objectives. As such, the information system should be construed in a manner that promotes improved performance and enhances the overall financial performance of the organisation.

From **Error! Reference source not found.**, it is observable that the greatest percentage of the respondents who participated in the study had a bachelor's degree (48%). It is also worth noting that at least 29% of the participants had a master's degree, 14% a doctorate degree, and 10% a College Diploma/Diploma of higher education. Essentially, a college diploma was the lowest qualification that was observed, and only 10% of the participants had such. This implies that the majority of the participants had at least a bachelor's degree and above, hence quite knowledgeable in their fields of specialisations and, specifically, information systems in the banking sector. It is vital to note that no participant mentioned to have the highest qualification of High school diploma/General Certificate of Secondary Education (GCSE)/Kenya Certificate of Secondary Education (KCSE) and also, not a single participant also mentioned to have the highest qualification of Post-high school certificate /General Certificate of Education Advanced Level. Banking Information systems deal with sensitive data, and hence it is

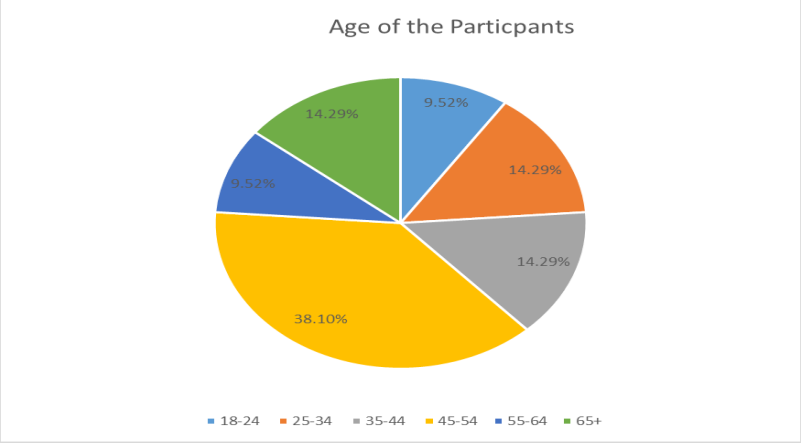

Fig. 3: Age of the participants

critical to ensure that the individuals credited with the responsibility of protecting the data and also overseeing organisational operations relevant to the storage and protection of the information resources are knowledgeable and well qualified [28].

The participants were once again asked about their working experience in a banking environment. This question was made to gauge how well the participants are versed with the banking sector. This question was made to gauge how well the participants understand the banking industry. Essentially, the more years of experience and individual has in a particular industry, the more he/she understand that particular industry [27]. In this case, substantial years of experience in the banking industry is capable of exposing the individual to trends with respect to data breaches, risk mitigations, market trends, financial performance, and strategic leadership of the respective organisation.

From the **Error! Reference source not found.**, it is clear that the majority of the participants had 3-10 years of experience in the banking industry, with 33.33% of them having 3-5 years and another 33.33% having 6-10 years. It is, however, critical to note that at least 19% of the participants had 11-15 years, while 4.8% had 16 years and above. On the same note, fresh entrants in the banking industry were 9.5%; this accounts for individuals with 0-2 years of experience in the industry.

The participants were once again asked about their perspective regarding risk avoidance with respect to their organisation's banking information system. The aim of the question was to elicit how prepared the Kenyan commercial banks are in preventing the materialisation of risks. Risk avoidance is a critical risk management strategy, which seeks to ensure the risk is avoided before it materialises [11]. In line with this, organisation management should ways seek to eliminate exposures, activities, and hazards that bear the ability to negatively affecting the organisational assets [41]. In order to evade vast financial adversities associated with threatening events, it is essential for a firm to come up with proactive risk avoidance strategies that are aimed at totally eliminating the threats. Bennett et al. consider risk avoidance as the first step toward optimal risk management [8].

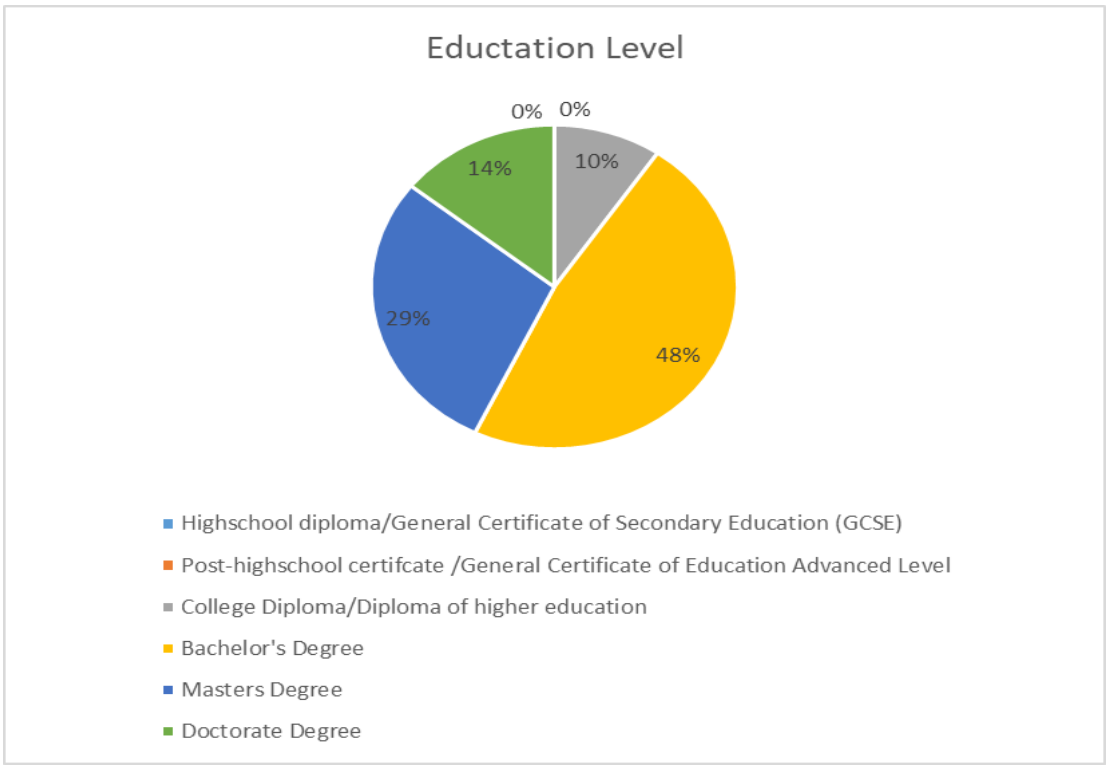

Fig. 4: Education level of the participants

Analysis of the participants' responses to 11 statements with respect to risk avoidance in their organisation is presented below.

1. My organisation has a strong Acceptable Use Policy
2. Punishment is issued to individuals who violate the Acceptable Use Policy
3. All new employees are trained regarding data security after recruitment
4. Data security is perceived as both collective and individual responsibility
5. There is ongoing retraining of employees on data security after a specific duration
6. I perceive the current organisational IT infrastructure to be up to date
7. All organisation workstations have up to date antivirus and internet protection

8. The IT department performs scheduled hardware maintenance of the IT infrastructure
9. The IT department performs regular updating of the servers and all PCs in the network
10. The customers and staff web and mobile applications are frequently checked for bugs and vulnerabilities
11. The customers and staff feedback on system issues are taken seriously and resolved with immediate effect

With respect to acceptable use policy, there were mixed reactions, with some participants' agreeing to their organisations having a strong acceptable use policy while other denying the existence of the same. Apparently, approximately 23.8% strongly disagreed, while another 23.18% disagreed as well. On the positive extreme, only 14.2% strongly agreed, followed by 28.5% agreement. Overly, the weighted average obtained was 2.86, which is basically on the negative extreme and below 3.0, which is the neutral position. This clearly indicates that the majority of the banks in Kenya do not have a strong Acceptable Use Policy. Lack of a well-founded Acceptable Use Policy in most cases crates vulnerabilities that can otherwise be taken advantage of by malicious individuals to propagate an attack on the information resources

As observable, despite a significant number of the banks lack a strong acceptable use policy, it was also unveiled that however weak or strong the policy is, individuals who violate it are usually punished. This can be derived from the high weighted average (3.67) that was obtained in this statement; this is towards the positive extreme and indicates an agreement with the statement. On the same point of view, it is also critical to note that a low disagreement rate was realised in this question, and specifically, only 4.76% of the participants took the strongly disagree position, while 14.29% took the disagree position. The majority of the participants (42.86%) took the agree position, while the reining 23.81% took the Strongly agree position. From this statement, it can be concluded that the Kenyan commercial banks take violation of the acceptable use policy very seriously.

With respect to training other new employees after recruitment, there was a mixed reaction, with

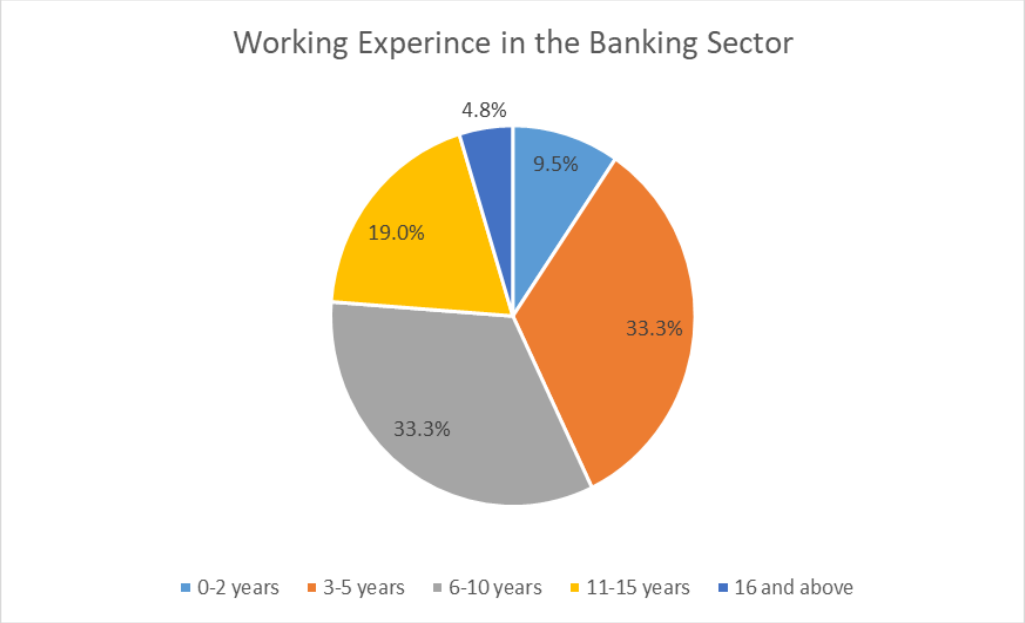

Fig. 5: Working experience of the participants in the banking sector

the majority of the participants (28.55%) taking a neutral position, while 23.81% is agreeing with the same. Nevertheless, a mean of 3.05 was obtained in this question, cauterised by a 1.25% standard deviation. This clearly indicates that while some banks train their new recruits on the essence of data security, others do not. The 3.05 neutral core ideates that training is averagely done by the Kenyan commercial banks for the new employees, specifically on how to protect the clients' data.

Data security in an organisational setting is basically a collective responsibility, and both employees and managers must strive to ensure that the organisational data is protected [25]. With a score of 3.29 and a standard deviation of 1.25, it is no doubt that the majority of the participants perceived data security as a collective responsibility. Nevertheless, it is also worth pinpointing the 9.52% who strongly disagreed and 19.52% who disagree don the same. This implies that in some banks, the employees still do not perceive information security as a collective responsibility. This creates a lapse in protecting data, an aspect that can lead to the development of vulnerabilities that can lead to data security threats. From the same point of view, it was

also established that retaining the employees is averagely done.

On a different note, with respect to the organisational IT infrastructure, it was unveiled that while some participants felt that their IT systems were up to date, others felt otherwise. This is supported by 14.29% who strongly disagreed, 19.05% who disagreed, another 19.05% who neither agreed nor disagreed, and 33.3% who agreed. Cumulatively, 33.25% of the participants took a negative stance on the issue. This resulted in a weighted average of 3.14, which is towards the neutral position. This implies that on average while some banks are using up to date technologies, others are not. Failure to use pirated technology creates loopholes that can otherwise be taken advantage of by malicious individuals. As outlined by Flores et al., old or obsolete technologies in most cases are associated with security lapses, which are not healthy for an information system [18].

The presence of antiviruses and internet protection in all organisation workstation is perhaps one of the statements on risk avoidance that received high positive feedback. In this statement, a weighted average of 3.67 was obtained, which is literally in the positive extreme and towards the agree position. This is supported by the fact that approximately 28.57% of the participants neither agreed nor disagreed, while the same percentage was also recorded in the agree and strongly agree positions. On the other hand, 4.76% strongly disagreed, and 9.52% disagreed. This implies that some banks still have out of date or antivirus and internet protection installed on their machines.

Scheduled hardware maintenance plays a critical role in protecting organisational data. Frequent hardware maintenance aids in preventing downtimes as well as system failures associated with IT infrastructure hardware issues. The responses scored in this question indicate 38.10% agreement and 19.05% strong agreement, characterised by a 3.38 weighted average and 1.25 standard deviation. The weighted average is above the neutral position and toward the positive extreme. This shows that the majority of the banks perform scheduled hardware maintenance; however, a significant number still does not perform any scheduled hardware maintenance. This then necessitates the need to carry out an investigation to establish why such institutions do not perform such scheduled maintenance and come up with a solution to the same. Conversely, there is a need for the IT department to ensure that the servers and PCs in the organisation network are updated in a timely version. The servers and pcs should be running the latest software update in order to evade any security risks that may be associated with obsolete or older versions of the software [7]. Banks deal with critical data and hence ensuring that all systems are up to date is out of the question. In this respect, the majority of the participants (23.81%) took a neutral position, while another 23.81% agreed. The minimum scores recorded were on the strongly disagree position, whereby only 14.29% of the participants took that position. A weighted average of 3.14 was obtained. The weighted average is slightly above the neutral position and toward the agreement position. This indicates that while more than half of the Kenyan commercial banks perform regular updating of their servers and the workstations, there is a significant number that does not do the same. This, in turn, creates data security laps which otherwise can predispose the organisation to unwarranted attacks

In order to ensure data protection and increase the risk avoidance level of banks, there is as well the need to frequently check for bugs and vulnerabilities in the applications that are used by both the organisation staff and the customers. In line with this, the applications should be monitored and frequently checked to unveil any potential security issues that need to be fixed. Risk avoidance in banking information security is all about ensuring that potential threats are eradicated. This statement received a relatively positive response, whereby the majority of the participants (38.10%) took the neutral position., 23.81% took the strongly agree position and 19.05% took the agree position. The recorded score resulted in a 3.38 weighted average and a standard deviation of 1.21. The weighted average is slightly above the neutral position, which indicates that more than half of the banks frequently check for vulnerabilities and bugs in the applications used by the customers and the staff. However, 19.4% still took the strongly disagree and disagree positions, indicating that the checking of vulnerabilities and bugs is not regularly done. As stipulated in the Kenyan Data Protection Bill of 2018 and Article 31 of the Kenyan Constitution, it is the duty of an organisation to protect its data from deliberate and accidental access by third parties [47], [48]. This can, however not be warranted if the applications used by the customers and the staff are not regularly checked for any security issues. This goes hand in hand with the ability of the IT personnel to ensure that the issues Raised by the staff and the customers with respect to the usability of the applications. Essentially, there should be a robust feedback system integrated into applications to ensure that the staff and customers can easily report any system issues. According to the study, the majority of the participants (28.57%) felt that feedback provided by the customers and staff regarding system issues is taken seriously. This was well supported by 19.05% who took the agree position. A vital point to note is however that 28.58% of the scores recorded were towards the negative extreme and shows that a significant number of banks do not take feedback raised by customers and staff on the application issues serious. With a weighted average of 3.33, a lot

needs to be done on the industry and enhance the response rate of the banks to customers' feedback.

Risk transference remains a vital risk management strategy that is commonly embraced by busies organisations. In the banking sector, there is a need to ensure that some risks are transferred to third parties in order to reduce the impact on the organisation should the risk materialise. Risk transference is often achieved through outsourcing/contracting of competent organisation to perform some activities for the purpose of the organisation. With respect to risk transference, the participants were as well asked a number of statements to establish how well the banks in the Kenyan financial industry have transferred some risks to third parties. The statements are given below:

1. My organisation often outsources IT services
2. Outsourced parties are held totally liable for any damage/ threat resulting from the outsourced service
3. The organisational policy regarding outsourcing/contracting is strongly followed
4. Contracted/ outsourced organisations' performance is closely monitored and evaluated
5. The outsourcing/contracting agreements have risk transfer agreements that obligate the contracted party

With respect to outsourcing the IT services, it was unveiled that the Kenyan commercial banks do not often outsource IT services. This is supported by the fact that from the figure 6, 19.05 % of the participants strongly disagreed, 38.10% disagreed, 19.05% neither agreed nor disagreed, 14.29% agreed and finally, 9.52% strongly agreed.

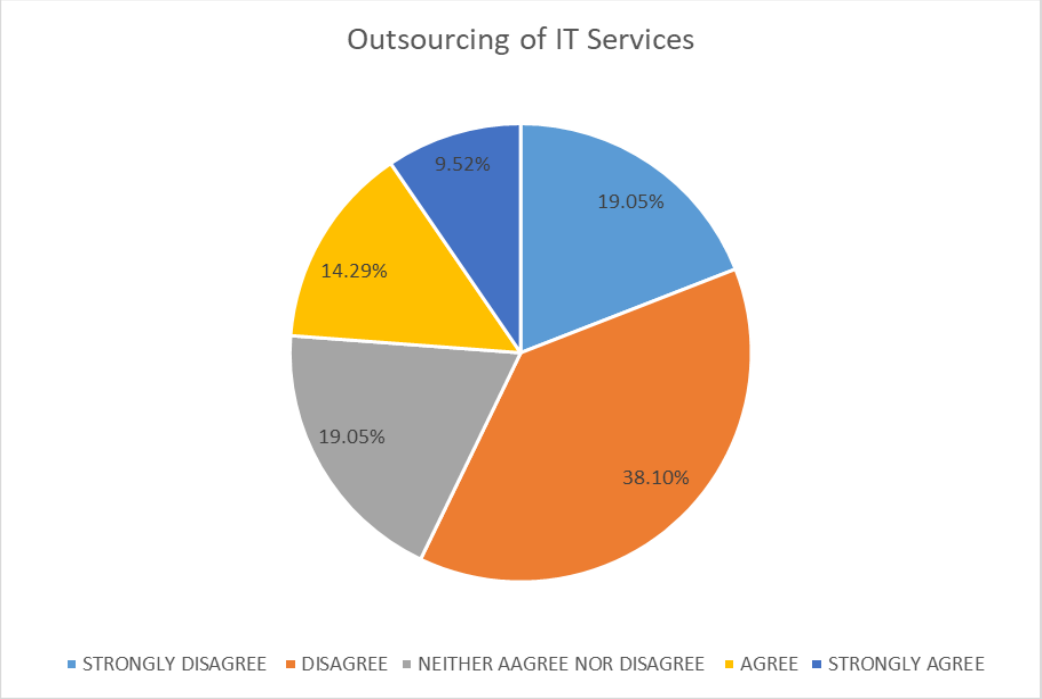

Fig. 6: Outsourcing of IT services by Kenyan commercial banks

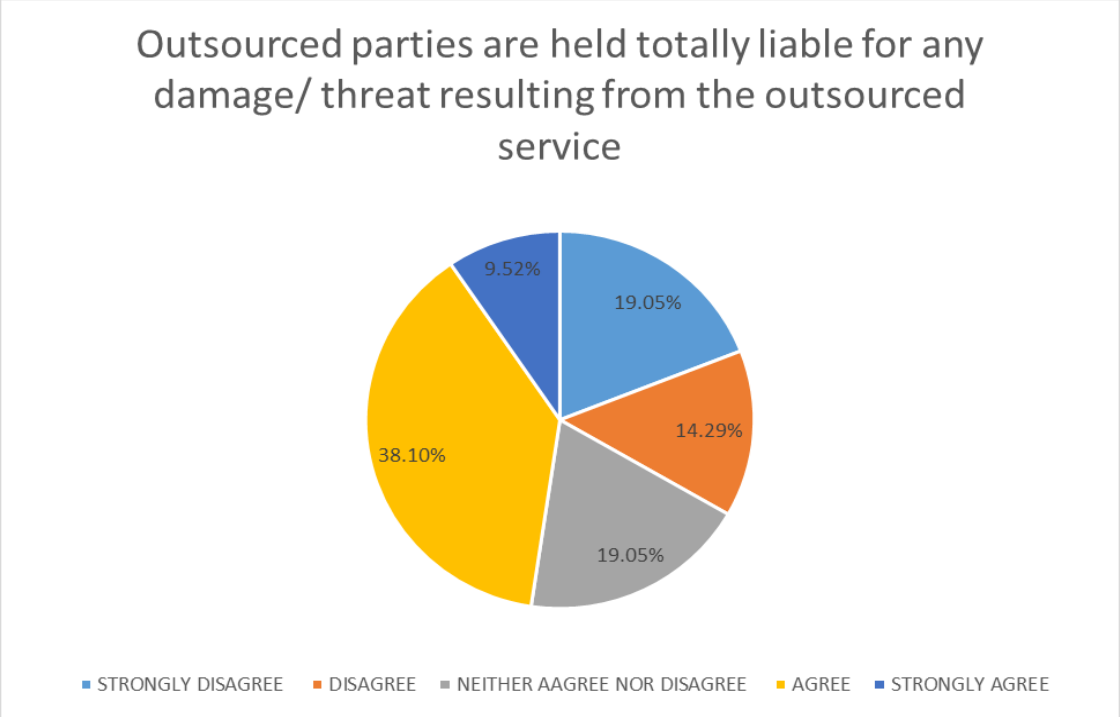

Fig. 7: Liability of the outsourced parties

A 2.57 weighted average was obtained in this question, which is below the neutral position and towards the negative extreme. This implies that the Kenyan commercial banks seldom outsource their services. While there could be a reason why the majority of the banks do not outsource, the latter still remains a critical risk management strategy that must be exploited at all cost outsourcing/contracting characterised by an agreement that is signed by both parties. Outsourcing is governed by various laws; the most fundamental are the agency and contract formation laws [15].

With respect to the outsourced parties being held totally liable for any damage/ threat resulting from the outsourced services, 38.1% of the participants agreed, followed by 19.05% who neither agreed nor disagreed. The strong agreement position came in the also, with a score of 9.52%. This is observable in figure 7. The weighted average noted was 3.05, with a standard deviation of 1.29.

This clearly implies that while approximately half of the banks have fully transferred the risks emanating from outsources services to the respective third party, others have limited risk insurance from the same and hence may be partially liable for damages resulting from the outsourced services. De Hae comments on the need for comprehensive insurance against the risk that emanates from outsourced services; according to the researcher, a firm should ensure limited to no liability on any damage that results from any adverse effects suffered from a service that is outsourced from a third party [16].

Integrated risk management is the most reliable strategy; however, under this approach, it is critical to ensure alignment of the risk management strategy with the corporate objectives and governance [9].

The organisation outsourcing/contracting policies should be followed to the latter. This ensures a limited deviation from the organisational strategies and promotes improved performance. In the case of banks in Kenya, highest scores (33.33%) were recorded in the strongly agree position, with the same scores being as well served in neither agree nor disagree position. This is well presented in figure 8.

With a weighted average of 3.81, the responses in this question clearly show that almost all banks in Kenya are strongly committed to adhering to their outsourcing policies. On the same note, the performance of the subcontracted firm must be closely monitored and supervised. This aids in eliminating any underperformance and out setting any activities that are carried out in manner that is not in one with the corporate objectives. The majority of the banks were found to closely monitor and evaluate the performance of the outsourced companies. This is supported by the fact that 33.33% agreed, 23.81% be neither agreed nor disagreed, and 19.05% strongly agreed as observable from figure 9.

The lowest score was recorded on the strongly disagree and disagree positions, which had a cumulative percentage of 19.04%. Factoring in the weighted average of 3.48, it is prudent to argue that more than half of the Kenyan commercial banks usually exercise monitoring of their subcontracted companies' performance in order to ensure that everything is the right track.

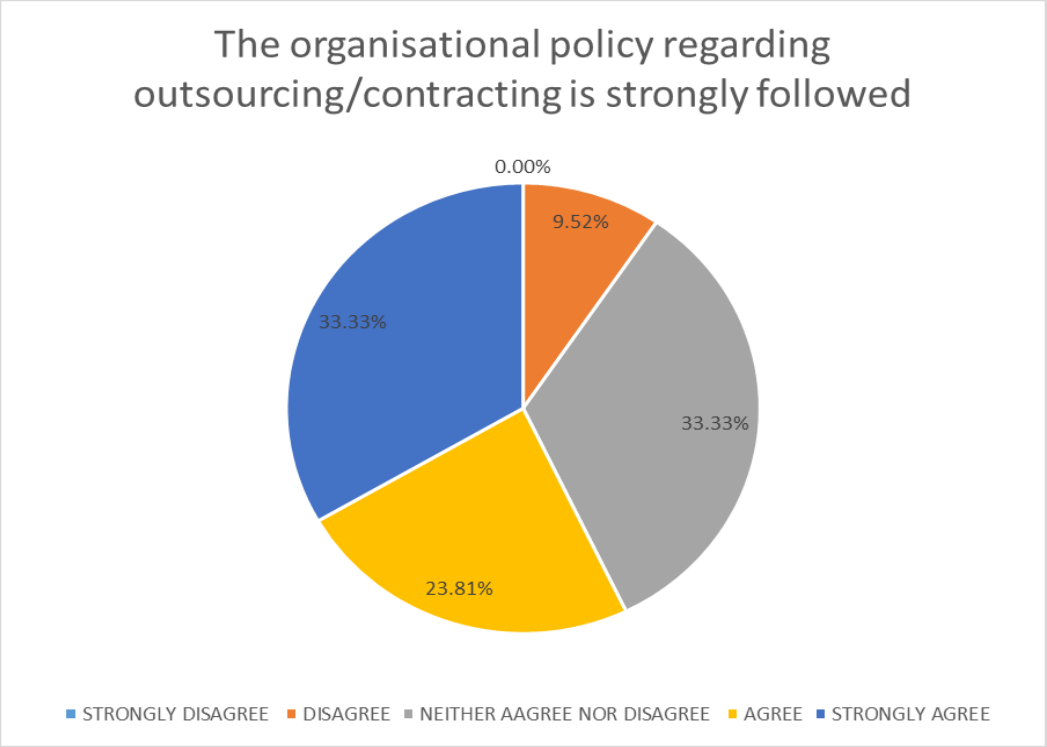

Fig. 8: Following of the outsourcing/contractual policies

In outsourcing, risk transfer agreement is an important element, as this indicates the extent to which subcontracted party is obligated. Just as earlier on mentioned, it is critical to ensure that the highest risk possible is transferred to the subcontracted party, as this forms part of the risk management strategies.

In connection with this, the responses from the participants unveiled that the Kenyan commercial banks' outsourcing contracts are characterised by risk transfer agreements that obligate the subcontracted party. This is because a mean average of 4.14 was obtained, due to the high percentage of participants who took a strong agreement position (57.14%). Nevertheless, a few cases of disagreement with the latter were noted, which implies that some Kenyan commercial banks ignore elements of explicit risk transfer agreements that obligate the subcontracted party (see figure 10).

Risk mitigation is the third facet of risk management investigated in the current study. The latter entails putting in place measures that are made to reduce the adverse effects that emanate from that materialisation of a specific risk. Any business organisations that wish to easily address its risk must come up with proper risk mitigation measures [43]. This is especially true for the risks that cannot be avoided or transferred. In the case of a data breach, the adverse effects include but not limited to destruction of data, using the data for fraudulent purposes, stealing of the data, blackmailing of the victims of the data breach, and finally, manipulation of the records.

In line with risk mitigation measures, it is critical for a firm to institutes strategies that are in line with the corporate objective and which are aimed at reducing the adversity of beaches. The statements are given below:

1. My organization has a disaster recovery plan
2. My organization responds to disasters affecting information system aptly
3. My organization updates the disaster recovery plan often
4. My organization has a team of experts dedicated to risk mitigation
5. My organization has an explicit business continuity plan
6. The business continuity plan is updated frequently
7. My organization's business continuity plan is actively supported by the top organization management
8. My organization has a robust incidence response plan
9. The incidence response plan is updated regularly to factor in changes in technology and technological trends
10. My organization has a team of experts dedicated to incidence recovery
11. My organization has an explicit policy on risk mitigation
12. The risk mitigation policy is regularly updated

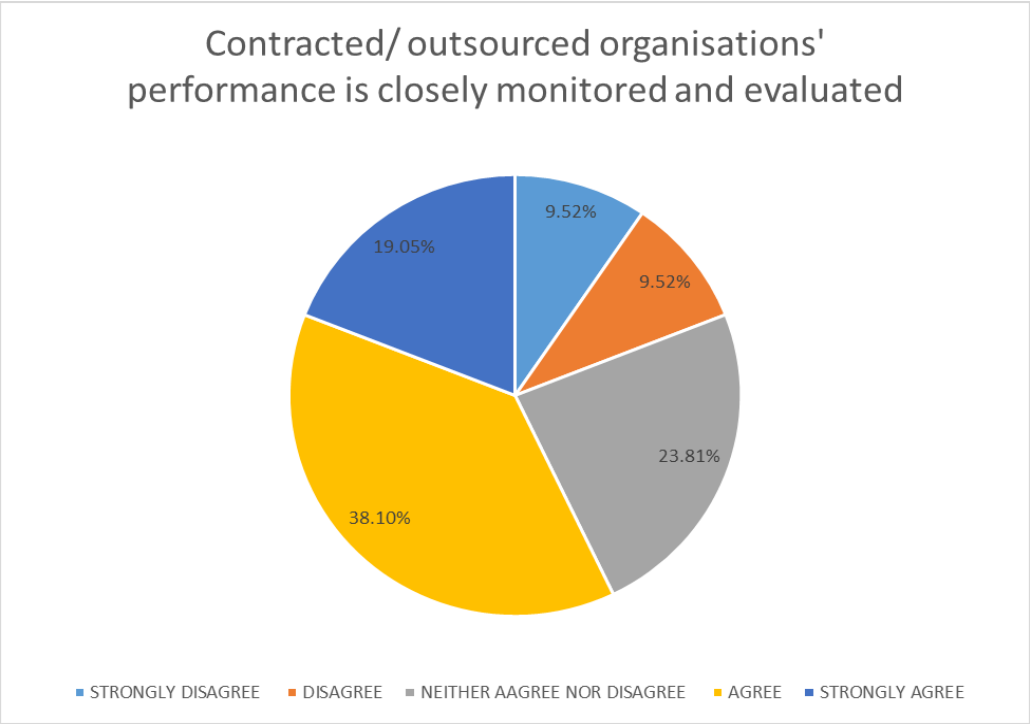

Fig. 9: Performance monitoring and evaluation of the contracted parties

With respect to the banks having a disaster recovery plan, it is quite worrying that out of the responses collected, only 28.57% agreed, and 9.52% strongly agreed. This is quite low compared to 14.29% strong disagreement and 28.57% disagreement. Overly, a weighted average of 2.9 was obtained, which is basically a neutral position indicating that while half of the banks in Kenyan commercial have a robust disaster recovery plan, others do not have. The scores recorded in this statement were as well reflected on the question of the bank's responsiveness to disasters, whereby a 3.14 weighted average was obtained. The majority of the participants (28.57%) neither agreed nor disagreed with their banks having a robust disaster response mechanism, while 23.81% agreed, and 19.005% strongly disagreed. The scores recorded on this statement shows that more than half of the banks in Kenyan commercial responds to disasters affecting information security aptly, while less than half than half do not respond aptly.

With respect to updating the data recovery plan, the majority of the participants (38.10%) agreed with the statement, while 14.29% strongly agreed. It is, however, worth noting that there was a 19.05% disagreement. The weighted average of 3.14 obtained is slightly above the neutral position of 3.0, which indicates that slightly more than half of the Kenyan commercial banks update their data recovery plan regularly while the rest do not.

The existence of a team dedicated to risk mitigation received high positive scores, with a weighted average of 3.62; this is probably due to the lack of scores on the strong disagreement position as with the majority of the scores (33.33%) being recorded on the neutral position, 28.57% on agreeing position and 23.81% on strongly agree position. The scores are well reflected in statement 12, whereby the participants were asked on whether the risk mitigating policy is regularly reviewed and updated. High scores were as well recorded, characterised by the cumulative percentage of 66.67% who either took the agree and strongly agree positions. It is, however, critical to not that 4.76 strongly disagreed, while 19.05% disagreed. This indicates that while some banks in Kenya occasionally review their risk mitigation policy, a significant number still does not perform a regular review and update of the same. Such an aspect may end up creating a loophole that can otherwise lead to organisation information system predisposition to data security threats.

A business continuity plan is a critical risk mitigation strategy that is often used by business organisations. The need for firms to have an explicit business continuity plan that is aimed at ensuring the continuity of business operations once an organisation is faced with adversity [8].

In the present study, the participants were asked whether their organisations had an explicit business continuity plan. It was established that at least 47.62% had an exploit business continuity plan, approximately 23.81% were neutral about the question while the rest had one explicit business continuity plan. On the same note, it was also found out that more than half of the bank's stills supported the business continuity plan that was in place.

Still, on risk mitigation, incidence planning was found to be a major problem, whereby 38.10% of the

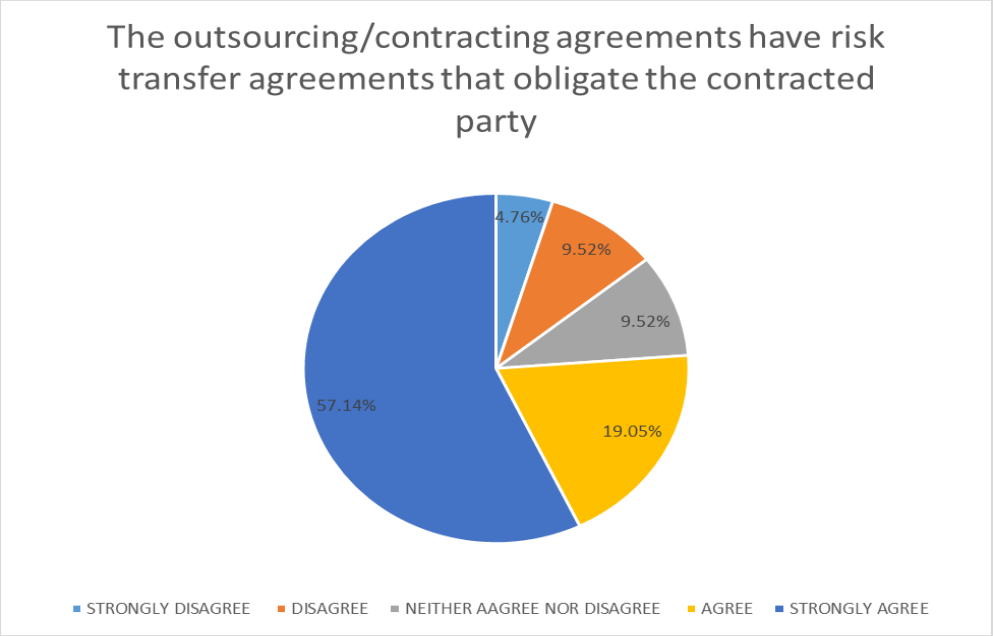

Fig. 10: Obligation of the contracted parties in risk transfer agreements

banks were found not to have a robust incidence response plan. Lack of a robust incidence plan creates significant information security lapse that may be taken advantage of by malicious individuals. Such cores can somewhat be used to explain the seemingly poor scores on the existence of an explicit policy on risk mitigation, whereby 19.05% of the participants took a negative position while only 9.52% took a neutral position. This then underpins the need to give the Kenyan banking institution the ensure the adoption of a strong risk mitigation policy.

Over the years, various organisations have been developed in an effort to develop the best practices in the industry. With respect to information system security, there are various institutions which develop guidelines that should be followed for effective in information security. These guidelines are often in line with various government regulations and are fully associated with some certifications to show that an organisation has complied with the given guidelines. While compliance is not an indicator that the information system does not contain any loophole, it shows that the organisation is making use of the best patriates in the industry, and hence has reduced chances of an information systems breach. 14 major organisations and agencies were identified globally, which aid in the development of information security related regulations as well as well as the issuance of

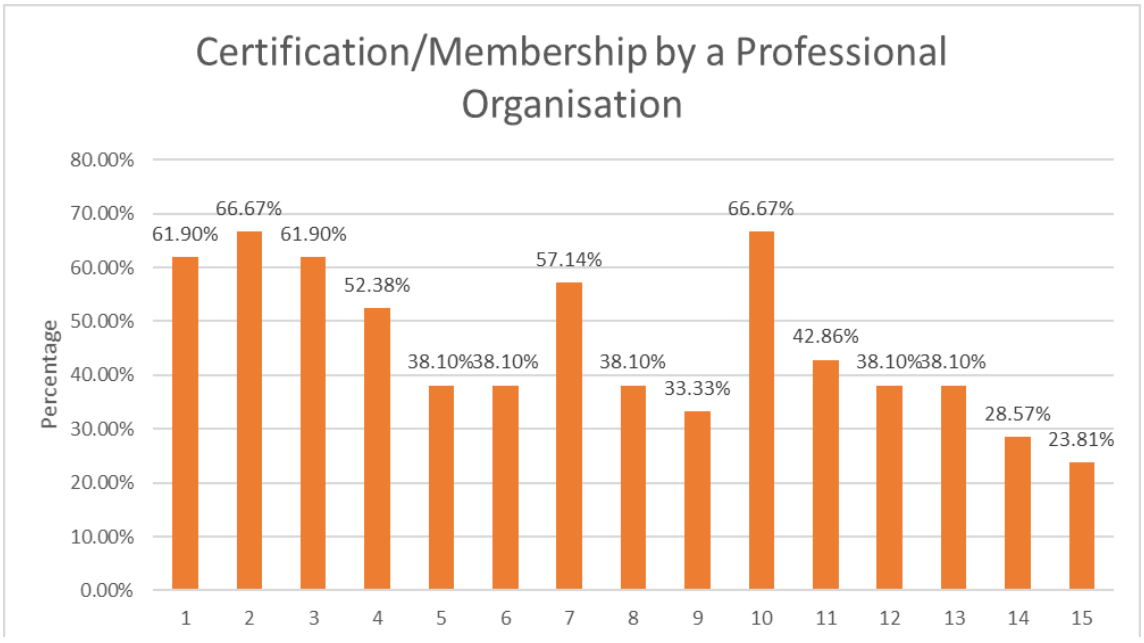

Fig. 7: Kenyan commercial banks' compliance with Kenyan government regulations and standards organization

certification for the organisations that are in compliance.

The certification/standards organisations are listed below:

1. ISACA - COBIT 5
2. ISO/IEC 27001 Information security management
3. Kenyan Data Protection Bill of 2018, and Article 31 of the Kenyan Constitution.
4. British Standards Institution (BSI)
5. SANS's Critical Security Controls for Effective Cyber Deafens
6. Information Technology Infrastructure Library essentials (ITL)
7. European Union Agency for Network and Information Security (ENISA)
8. Cyber Management Alliance
9. CREST
10. Bureau Veritas Certification
11. Knox Cyber Security
12. Ultima Risk Management (URM) Limited
13. Xyone Cyber Security
14. Tranchulas

Owing to this, the participants in the current study were asked to identify whether their operations are in line with all or some of the agencies. From figure 11, is observable that the operations of 66.67% of the banks operating in Kenya were in compliance with ISO/IEC 27001 Information security management and the ITL. This implies that someway somehow, 33.33% of the banks operate in a manner that does not conform to the ITL essentials and ISO/IEC 27001. 61.90% of the Kenyan banks were however in compliance with COBIT 5 guidelines set forth by ISACA, as well as the Kenyan government Data Protection Bill of 2018 and Article 31 of the Kenyan Constitution. This implies that still, 38.10% of the banks in Kenya operate in a manner that does not comply with the government regulations in one way or another.

Essentially, the failure of banks to comply with such regulations and guidelines creates some security lapse that culminates into unwarranted risks. Tranchulas had a minimum membership of 23.81%. Generally, there is the need to encourage compliance with the best practices in the industry set forth by the standards organisation, as well as compliance with the government regulations.

Finally, with respect to the safety of data, 71.35% of the Kenyan banks have not experienced a data breach in the last 5 years (See **Error! Reference source not found.**). In turn, 28.65% of the banks have experienced a data breach in the last five years. Such an aspect implies that data security is still an active risk area that must be addressed. The fact that there have been cases of a data breach is perhaps the reason why a substantial percentage of the respondents believed the data held by their banking situations was not safe. According to the study, 9.52% of the participants strongly disagreed that the data held by their organisation was safe while still. 19.05 disagreed. This implies that the safety of data held by a number of Kenyan banks is quite questionable

Security breaches should not be underrated, regardless of their impact. Technology is increasing by the day, and some Kenyan banks are not keeping up with the pace as outset in the study. As a result,

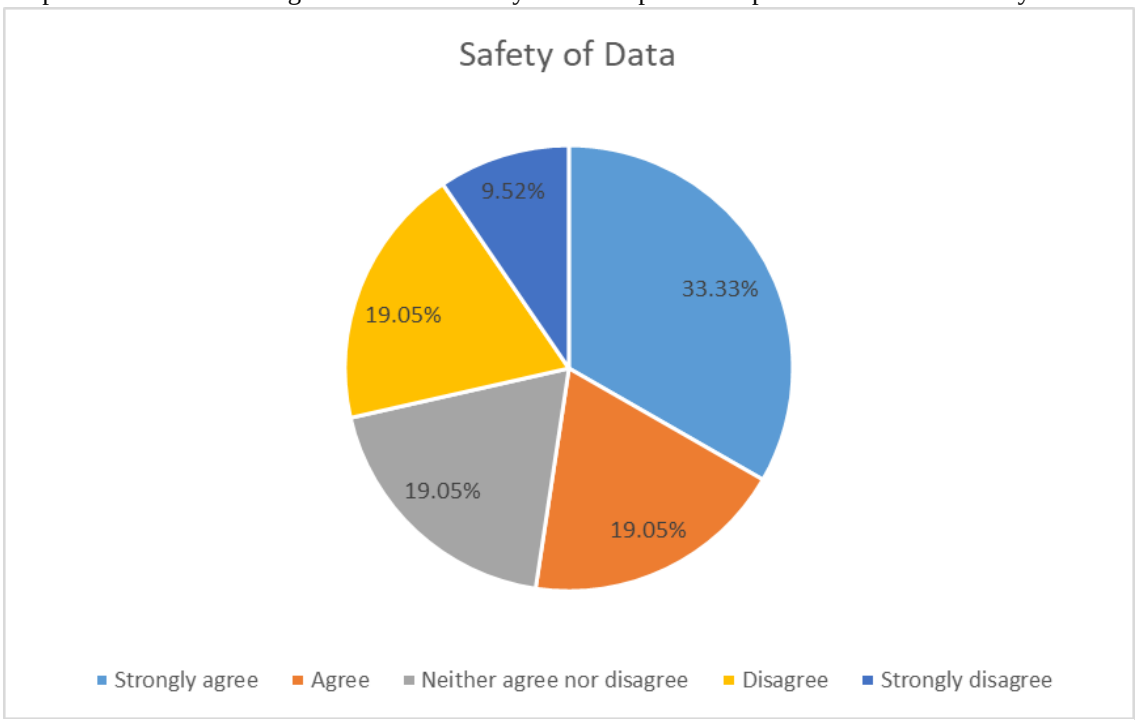

Fig. 12: Safety of banking data in Kenya

their information systems become outdated, thus creating many loopholes that hackers might take advantage of. This is supported by the fact that, according to the study approximately 28.65% of Kenyan commercial banks have suffered a data breach over the last five years. When an intruder infiltrates a database, they are able to access information pertaining to the strategies of the organisation or other sensitive information that can jeopardize organisation operations as well as reduce the trust of the customers on the organisation [46]. As presented in 2 below, 9.52% of the participants strongly disagreed that the data held by their organisation was safe while still. 19.05% disagreed with their data being safe. Kenyan commercial banks therefore need, ensure that their information and the information of their customers is well stored in reducing the negative financial impact of security breaches

Risk management remains to be one of the prime areas that can greatly aid in managing information security breaches. As observed in the literature, risk management covers three main facts, which include avoidance, transference, and mitigation. intentional or inadvertent exposure of information to unintended persons has become one of the most critical components to the contemporary organisations [13]. Firms are finding it difficult to protect data against information leakage in the era of big data prompting data to become one of the most critical components of an enterprise, managing, and analysing large amounts of data [14]. The authors find that data management and protection is an element that provides an organisation with an enormous competitive advantage. The analysis shows that the Kenyan commercial banks are yet to fully ensure the three dimensions of risk management are well covered; therefore, risk management still remains an area of concern.

VI. DISCUSSION

Cyber risk has become a contested issue over the recent past. Technological advancements have not only positively influenced how people and institutions operate but have also presented major issues that seem to affect everyone [35]. The issue of data security has affected all economical sectors and negatively affected their financial performance. Further, even though the internet is the new platform on which businesses are becoming successful, the increase in its usage has increased the vulnerabilities of the infrastructures that have been put in place in conducting businesses [35]. The increase in these vulnerabilities has made it possible for people with ill intent to access the information systems of these institutions and access information without using the proper channels. Once an intruder infiltrates into the information systems of an organisation, their actions can adversely affect the operations of the organisation

Once a security breach occurs, it implies that some individual has infiltrated the information systems and action needs to be taken. Once the organisation realises that its information systems have been infiltrated, they may decide to install new infrastructure or investigate the loopholes within their systems that the hacker might have used in their infiltration [23]. A complete overhaul of the information systems within an organisation translates to implicit costs, which affect the financial reports of the organisation. The implicit costs of security breaches are way much higher than anticipated, which affects the financial reporting of the organisation [22]. When such implicit costs become more recurrent, they can usually have an adverse negative impact on the future of the organisation in the market.

A business is usually established with the main aim of making profits and increasing the wealth of the shareholders. As such, all activities in the organisation must be construed towards promoting the best interest of the shareholders and increasing the organisational performance. Protecting the stored data is a critical activity that bears the ability to affect the overall organisation performance. The discussion on the impact of an information system is paramount, and the ripple effects are conspicuous. companies that self-report their security posture as superior and have swift actions towards the breach recovered their stock value within a short period as compared to companies with poor information society that suffer stock price declines for a substantial period [30]. Strong information system investment was also associated with high consumer and investor trust [5].

The impact of enterprise information security risk can be countered through DLPD (Data Leak Prevention and Detection Techniques) approaches [13]. DLPD forms a critical risk avoidance technique that can be adopted by the Kenyan commercial banks as it was outset that approximately 31.67% do not have comprehensive risk avoidance techniques. The core purpose of DLPD is to identify, monitor, and protection of privy data from unauthorised access and project any potential leakage. DPLD approaches are classified into basic security measures and designated DLPD approaches [14]. Basic security measures include approaches such as security data publishing, encrypting, and enforcing access rights to sensitive data and are critical in safeguarding data at rest, which is the first line of data leak prevention. The DPLD strategies provide more confidence to investors and customers since they are guaranteed of information security [13], [14]. Investor and customer confidence is a paramount element of enhancing positive financial performance within an organisation.

The Kenyan commercial banks are yet to fully roll out robust risk management strategies, with the majority lagging in the implementation of risk avoidance, transference, and mitigation strategies.

Information system breach has a negative impact on the financial performance of an organisation. The implications of a data breach are many, including but not limited to increased customers' litigation tainted brand image and reduced performance of the firm in both short term and long term. For instance, Arcuri et al. noted that cybercrimes cost the global economy approximately $450 billion each year and that the attacks are becoming more frequent and enormous [4]. A data breach cost IBM $ 4 million in the year 2016 [14]. All these costs implications lead to financial losses, and as Rajakumar and Shanti noted, they can halt the business operations in its entirety [32]. This implies that if the Kenyan commercial banking continue operating as per their current procedures, there are increased risks of cyber-attacks on their information system because as denoted from the study, the data held by 28.57% of the banks are not safe, a figure that most definitely associated with the fact that 28.65% Kenyan commercial banks that have faced data breach in the last five years. On the same note, the fact that 33.33% of the banks have not complied with the ITL and still, 38.10% are yet to comply with the U Kenyan government Data Protection Bill of 2018, and Article 31 of the Kenyan Constitution indicates that much has to be done in order to establish the reason for under compliance.

There is a statistically significant negative impact of breaches in security in a company`s market value in the first ten days after an announcement of a security breach has been made [46]. Hovav and Gray explained the observation by stating that investors are usually wary of cases relating to security breaches, which is why they would withdraw their investments from a company once such cases have been announced [20]. Even though Martin et al. note that the information on economics information security is limited, the willingness of investors to invest in a company is affected by the information in the public domain on how the organisation is faring [23]. If the public has negative information concerning an organisation, the chances are minimal that the investors would be willing to invest in a particular organisation.

The relationship between a firm and its customers is one of the factors that determine its financial performance. An organisation should be in a position to relate positively to the customers and ensure that their needs are met [37]. When customers shop using their credit or debit cards, their personal information is stored in the organisation`s database [28]. In case of a security breach, attackers are sometimes able to access the personal information of the customers, which they can use for malicious purposes. The reaction to security breaches is usually instant, and most of them would opt for alternative organisations in the market [25].

Security breach affects the brand image of an organisation. Even though customers and potential customers might not understand the reasons behind the breach, the breach sends a clear message that it cannot be entrusted with its customers` personal information. The perception of the public affects an organisation, and in a case of security breach, the public would have a negative perception towards the organisation [38]. An announcement of a security breach in an organisation is perceived as a show of how the organisation is ineffective in its operations. Current and potential customers would, therefore, shy away from the products or services offered by the organisation, which would largely affect the sales and financial performance of the organisation.

The biggest data breach risk found was the lack of sufficient risk avoidance measures, as well as the fact that the majority of the Kenyan commercial banks are reluctant to transfer some risks to third parties through outsourcing as 57.15 % of the participants disagreed to outsourcing IT services, while only 28.10% agreed; the rest of the participants took a neutral position. Essentially, the more an organisation is predisposed to data breach threats, the more it's financial performance is harmed whenever the risk materialises and the lesser attractive it becomes to the investors. Essentially, true economic effects are usually reflected in the security prices of the affected firm when the market is absolutely rational. It is also important to note that the study conducted the research on two types of companies; those that have experienced the security breach and those that have not experienced the breach. The study established for the organisation that had faced a data breach in the past, the IT managers still believed that, to a greater extent, the stored data was not safe.

VII. CONCLUSION

Cyber risk has become a contested issue over the recent past. Technological advancements have not only positively influenced how people and institutions operate but have also presented major issues that seem to affect [35]. The issue of data security has affected all economical sectors and negatively affected their financial performance. Even though the internet is the new platform on which businesses are becoming successful, the increase in its usage has increased the vulnerabilities of the infrastructures that have been put in place in conducting businesses [35]. The increase in these vulnerabilities has made it possible for people with ill intent to access the information systems of these institutions and access information without using the proper channels. Once an intruder infiltrates into the information systems of an organisation, their actions can adversely affect the operations of the organisation

Once a security breach occurs, it implies that some individual has infiltrated the information systems and action needs to be taken. Once the organisation realises that its information systems have been infiltrated, they may decide to install new infrastructure or investigate the loopholes within their

systems that the hacker might have used in their infiltration [38]. A complete overhaul of the information systems within an organisation translates to implicit costs, which affect the financial reports of the organisation. The implicit costs of security breaches are way much higher than anticipated, which affects the financial reporting of the organisation [23]. When such implicit costs become more recurrent, they can usually have an adverse negative impact on the future of the organisation in the market.

The impact of enterprise information security risk can be countered through DLPD (Data Leak Prevention and Detection Techniques) approaches [13]. DLPD forms a critical risk avoidance technique that can be adopted by the Kenyan commercial banks as it was outset that approximately 31.67% do not have comprehensive risk avoidance techniques. The core purpose of DLPD is to identify, monitor, and protection of privy data from unauthorised access and project any potential leakage. DPLD approaches are classified into basic security measures and designated DLPD approaches [14]. Basic security measures include approaches such as security data publishing, encrypting, and enforcing access rights to sensitive data and are critical in safeguarding data at rest, which is the first line of data leak prevention. The DPLD strategies provide more confidence to investors and customers since they are guaranteed of information security [14]. Investor and customer confidence is a paramount element of enhancing positive financial performance within an organisation.

The Kenyan commercial banks are yet to fully roll out robust risk management strategies, with the majority lagging in the implementation of risk avoidance, transference, and mitigation strategies. Information system breach has a negative impact on the financial performance of an organisation. The implications of a data breach are many, including but not limited to increased customers' litigation tainted brand image and reduced performance of the firm in both short term and long term. For instance, Arcuri et al. noted that cybercrimes cost the global economy approximately $450 billion each year and that the attacks are becoming more frequent and enormous [4]. All these costs implications lead to financial losses and can halt business operations in its entirety [32]. This implies that if the Kenyan commercial banks continue operating as per their current procedures, there are increased risks of cyber-attacks on their information system because as denoted from the study, the data held by 28.57% of the banks are not safe, a figure that most definitely associated with the fact that 28.65% Kenyan commercial banks that have faced data breach in the last five years. On the same note, the fact that 33.33% of the banks have not complied with the ITL and still, 38.10% are yet to comply with the Kenyan government Data Protection Bill of 2018, and Article 31 of the Kenyan Constitution indicates that much has to be done in order to establish the reason for under compliance.

There is a statistically significant negative impact of breaches in security in a company`s market value in the first ten days after an announcement of a security breach has been made [46]. Investors are usually wary of cases relating to security breaches, which is why they would withdraw their investments from a company once such cases have been announced [20]. Even though the information on information security is limited, the willingness of investors to invest in a company is affected by the information in the public domain on how the organisation is faring [23]. If the public has negative information concerning an organisation, the chances are minimal that the investors would be willing to invest in a particular organisation.

The relationship between a firm and its customers is one of the factors that determine its financial performance. An organisation should be in a position to relate positively to the customers and ensure that their needs are met [37]. When customers shop using their credit or debit cards, their personal information is stored in the organisation`s database [28]. In case of a security breach, attackers are sometimes able to access the personal information of the customers, which they can use for malicious purposes. The reaction to security breaches is usually instant, and most of them would opt for alternative organisations in the market [24].

The biggest data breach risk found was the lack of sufficient risk avoidance measures, as well as the fact that the majority of the Kenyan commercial banks are reluctant to transfer some risks to third parties through outsourcing as 57.15 % of the participants disagreed to outsourcing IT services, while only 28.10% agreed; the rest of the participants took a neutral position. Essentially, the more an organisation is predisposed to data breach threats, the more it's financial performance is harmed whenever the risk materialises and the lesser attractive it becomes to the investors. Essentially, true economic effects are usually reflected in the security prices of the affected firm when the market is absolutely rational. It is also important to note that the study conducted the research on two types of companies; those that have experienced the security breach and those that have not experienced the breach. The study established for the organisation that had faced a data breach in the past, the IT managers still believed that, to a greater extent, the stored data was not safe.

VIII. RECOMMENDATIONS

The following recommendations can aid in bolstering the risk mitigation measures employed by the Kenyan commercial banks in combating the adversities associated with a data breach.

First, the Kenyan commercial banks can increase their risk avoidance and transference rates, whereby approximately 57.15% were found to be least

interested in outsourcing and sharing information technology related services. Appan and Bacic investigated the impact of trade associations or sharing information technology with other competing firms on its financial performance [3]. Trade associations are referred to as the mechanisms that create an environment for exchanging and sharing information within an industry. Accordingly, sharing information system measures and practices help the participating members to adopt an oligopolistic market perspective, gain political and social influence, and enhance a specific regulation [3]. Apparently, the prime belief is that information sharing helps the firm to gain market control and benefit economically. As such, information sharing by the Kenyan commercial banks can as well results in reducing the propensity of information system breach, and it had a positive impact on the organisation performance.

Secondly, developing and implementing a robust and comprehensive business disaster recovery plan, incidence response plan, and continuity plan. This is a significant weakness for approximately 31.87% banks in Kenya, which were found to have poor risk mitigation measures. The utmost consequence of lack of a robust risk mitigation strategy is that the latter can result in grounded business operations should the risk materialise [32]. The losses incurred in case of a security breach hinder the prosperity of a business entity. An integrated mitigation system has more positive impacts as compared to a single system. This can entail a combination of risk avoidance, transference and mitigation measures with a specific team dedicated to executing either or all of the three when necessary

Thirdly an elemental method of mitigating information breach and the associated financial losses is by building a strong and effective system architecture as a way of avoiding information security breach risks. The system architecture begins with worm propagation where IP addresses of computers to obtain all the information about the vulnerable computer in the network are randomly scanned. After that, the system encompasses countermeasures, whose main agenda is to eliminate the dynamic worms and to trace the source of the breach. The countermeasures are done through an integrated analysis system known as IP traceback [29].

ACKNOWLEDGMENT

The researcher would wish to acknowledge every single individual who participated in the study. Your effort contributed to the success of this study. The results are a substantial step in developing better data-breach management strategies.

REFERENCES

[1] Alanezi, F., & Brooks, L. (2014). Combatting online fraud in Saudi Arabia using the general deterrence theory (GDT).

[2] Angst, C. M., Block, E. S., D'arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. MIS Quarterly, 41(3), 893-916.

[3] Appan, R. & Bacic, D. (2016) Impact of information technology (IT) security information sharing among competing for IT firms on financial performance: An empirical investigation. Communications of the association for information systems, 39(12), 214-241

[4] Arcuri, M., Brogi, M. & Gandolfi, G. (2015). How does cybercrime affect firms? The effect of information security breaches on stock returns. Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy. Retrieved from: http://ceur-ws.org/Vol-1816/paper-18.pdf

[5] Ashford, W. (2017). A strong cybersecurity posture reduces the impact of breaches. Retrieved from: https://www.computerweekly.com/news/450419072/Strong-cyber-security-posture-reduces-impact-of-breaches

[6] Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & management, 51(1), 138-151.

[7] Bell, B. G., Ndje, Y. J. & Lele, C. (2015). Information systems security management: optimized model for strategy, organisation, operations. American Journal of Control Systems an Information Technology, (1), 22.

[8] Bennett, J., Stager, M., Shevlin, G., & Tang, W. (2013). U.S. Patent No. 8,516,594. Washington, DC: U.S. Patent and Trademark Office.

[9] Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. Long range planning, 48(4), 265-276.

[10] Bryman, A. (2015). Social research methods. Oxford university press.

[11] Cardona, O. D. (2013). The need for rethinking the concepts of vulnerability and risk from a holistic perspective: a necessary review and criticism for effective risk management. In Mapping vulnerability (pp. 56-70). Routledge.

[12] Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organisational investment in information security control resources. Information & Management, 52(4), 385-400.

[13] Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralisation techniques and general deterrence theory. Computers in Human Behavior, 38, 220-228.

[14] Cheng, L., Liu, F. & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. WIREs, 7(5)

[15] Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2014). Future directions for behavioral information security research. computers & security, 32, 90-101.

[16] De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. Journal of Information Systems, 27(1), 307-324.

[17] Dwivedi, Y. K., Wastell, D., Laumer, S., Henriksen, H. Z., Myers, M. D., Bunker, D., ... & Srivastava, S. C. (2015). Research on information systems failures and successes: Status update and future directions. Information Systems Frontiers, 17(1), 143-157.

[18] Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organisations: Investigating the effect of behavioral information security governance and national culture. Computers & Security, 43, 90-110.

[19] Horne, C., Ahmad, A., & Maynard, S. (2016). A Theory on Information Security. Australasian Conference on Information Systems, 2016. Wollongong, Australia
[20] Hovav, A., & Gray, P. (2014). The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. CAIS, 34, 50.
[21] Kostopoulos, K., Papalexandris, A., Papachroni, M., & Ioannou, G. (2011). Absorptive capacity, innovation, and financial performance. Journal of Business Research, 64(12), 1335-1343.
[22] Martin, K. D., & Murphy, P. E. (2017). The role of data privacy in marketing. Journal of the Academy of Marketing Science, 45(2), 135-155.
[23] Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36-58.
[24] Martins, C., Oliveira, T., & Popovič, A. (2014). Understanding Internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application. International Journal of Information Management, 34(1), 1-13.
[25] Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. Journal of Operations Management, 35, 21-39.
[26] Nagin, D. S., Cullen, F. T., & Jonson, C. L. (2018). Classical Theory: The Emergence of Deterrence Theory in the Age of Enlightenment. In Deterrence, Choice, and Crime, Volume 23(pp. 13-38). Routledge.
[27] National Research Council. (2013). Education for life and work: Developing transferable knowledge and skills in the 21st century. National Academies Press.
[28] Nofer, M., Hinz, O., Muntermann, J., & Roßnagel, H. (2014). The economic impact of privacy violations and security breaches. Business & Information Systems Engineering, 6(6), 339-348.
[29] Periyasamy, S. & Duraiswamy, K. (2013). A proficient traceback approach using provincial locality aspects to eliminate denial of service attacks. J. Comput. Sci., 9, 271-276.
[30] Ponemon. (2010). 2009 annual study: US cost of a data breach. Retrieved from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_01220 9_sec.pdf
[31] Prajogo, D., Toy, J., Bhattacharya, A., Oke, A., & Cheng, T. C. E. (2018). The relationships between information management, process management, and operational performance: Internal and external contexts. International Journal of Production Economics, 199, 95-103.
[32] Rajakumar, M. & Shanthi, V. (2014). A security breach in trading system-countermeasure using IPTracedback. American Journal of Applied Sciences, 11(3), 492-498
[33] Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organisations. Computers & Security, 53, 65-78.
[34] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organisations. Computers & Security, 56, 70-82.
[35] Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. Information & Computer Security, 24(1), 73-92.
[36] Sen, R., & Borle, S. (2015). Estimating the contextual risk of a data breach: An empirical approach. Journal of Management Information Systems, 32(2), 314-341.
[37] Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs a more holistic approach: A literature review. International Journal of Information Management, 36(2), 215-225.
[38] Spanos, G., & Angelis, L. (2016). The impact of information security events on the stock market: A systematic literature review. Computers & Security, 58, 216-229.
[39] Taylor, S. J., Bogdan, R., & DeVault, M. (2015). Introduction to qualitative research methods: A guidebook and resource. John Wiley & Sons.
[40] U.K Government (2018). The Data Protection Act. Retrieved from https://www.gov.uk/data-protection
[41] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.
[42] Wortley, R., & Sidebottom, A. (2017). Deterrence and Rational Choice Theory. Juvenile Delinquency and Justice, 1-6.
[43] Wu, D. D., Chen, S. H., & Olson, D. L. (2014). Business intelligence in risk management: Some recent progresses. Information Sciences, 256, 1-7.
[44] Zafar, H., Ko, M. S., & Osei-Bryson, K. M. (2016). The value of the CIO in the top management team on performance in the case of information security breaches. Information Systems Frontiers, 18(6), 1205-1215.
[45] Conklin, W. A., & Dietrich, G. (2008, January). Systems theory model for information security. In Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) (pp. 265-265). IEEE.
[46] Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. Journal of Operations Management, 35, 21-39.
[47] P[arliamane of Kenya. (2018). The data protection bill, 2018: Arrangement of clause. Retrieved from http://www.parliament.go.ke/sites/default/files/2017-05/Data_Protection_Bill_2018.pdf
[48] Privacy International. (2019). State of Privacy Kenya. Retrieved from https://privacyinternational.org/state-privacy/1005/state-privacy-kenya
[49] Central Bank of Kenya. (2018). Central bank of Kenya directory of licensed commercial banks, mortgage finance institutions and authorized non-operating holding companies. Retrieved from
[50] https://www.centralbank.go.ke/wp-content/uploads/2017/05/Directory-of-Licenced-Commercial-Banks-Mortgage-Finance-Institutions-and-NOHCs.pdf