Effect of cybersecurity risk management practices on performance of insurance sector: A review of literature

Ben Kajwang (a)*

(a) PhD, Chartered Insurer, Chief Executive Officer, College of Insurance, Nairobi, Kenya

ABSTRACT

Cybersecurity is a set of technologies, processes, practices, and response and mitigation measures aimed at ensuring the confidentiality, integrity, and availability of networks, computers, programs, and data against attack, damage, or unwanted access. Cyber security risk management strategies include limiting data access to avoid putting sensitive information at risk. The purpose of the study therefore is to evaluate the effect of cybersecurity risk management practices on performance of insurance sector. A desktop literature review was used for this purpose. Relevant seminal references and journal articles for the study were identified using Google Scholar. The inclusion criteria entailed papers that were not over 10 years old. According to the findings, detected cyber risks need to be properly addressed in order to prevent secondary impacts that lead to vulnerabilities that interfere with the life of insurance institutions and the well-being of their customers. In addition, the study concluded that insurance industry performance can be improved through the implementation of cybersecurity risk management practices. Since it has been found that cybersecurity risk management strategies have a positive and significant impact on the performance of the insurance sector, the research recommends that insurance companies increase their use. Additionally, financial institutions ought to have funds set aside specifically for the purpose of facilitating the retention of risks, in the event that these risks actually materialize. In addition, the research suggests that insurance companies reorganize their product lines or establish premiums that are competitive in order to reduce the threat posed by their rivals and, as a result, prevent the loss of customers to those rivals. The research further suggests that insurance companies adopt appropriate product pricing in line with estimated risk, as this will ultimately lead to increased profitability.

* Corresponding author.

Introduction

Technology-based solutions are being adopted by organizations around the world, making the world a digital place. Because of this, the risk of cybercrime has increased, and this is especially true if the controls that are in place are insufficient or nonexistent. Incidents involving cyber risk can have a diverse range of effects on the businesses that are impacted by them. According to the Allianz Risk Barometer for 2019 and 2020, cyber risk, in conjunction with business interruption that is primarily caused by cyber risk occurrences, has been identified as the most critical risk facing businesses around the world. The practices of cybersecurity risk management help the insurance industry perform better by increasing client trust and strengthening data security and privacy, which ultimately leads to more potential for revenue, (Gatzert & Schubert, 2022).

Cyber risk is the potential for loss or harm as a result of compromising an organization's technological infrastructure. Cyber risk is associated with online activity, electronic commerce, information systems, networks, and data storage, and it refers to the potential for these things to be compromised (RSA, 2016). Threats and incidents related to cybersecurity are seen as having a greater potential for harm by larger companies, and as a result, adequate investments are made in the development of countermeasures. During the course of the last decade, cyberattacks on insurance companies have undergone a dramatic transformation as a result of the rise in...
their level of technical sophistication, frequency, and severity. Even though the majority of insurance companies have put in place a high level of cyber security precautions, the number of cyber-attacks continues to rise. This not only demonstrates the inevitability of cyber-attacks, but also the difficulty of completely guaranteeing the integrity of financial systems in insurance companies. More than half of the world's commercial banks have been the target of at least one type of cyberattack, as stated by Security Intelligence Solutions (2020).

The primary objective of cybercrime is to cause disruption to normal business operations as well as essential infrastructure. Data that has been illegally obtained is frequently utilized by cybercriminals for the purposes of financial gain, the infliction of financial loss, the damage of a person's reputation, the accomplishment of military objectives, or the dissemination of religious or political ideologies. Some hackers don't require a justification to hack; rather, they do it solely for the purpose of demonstrating their expertise. The adversaries are currently employing more cutting-edge strategies in order to target the systems. Everyone from sole proprietors to multi-national corporations and everything in between is impacted. Because of this, each of these companies has realized the significance of maintaining a high level of cyber security and is actively working to put into place all of the preventative measures that are currently available to ward off potential cyberattacks, (Tariq, 2018).

As a result of the rapid pace at which businesses are implementing digital transformations with the help of mobile devices, cloud services, social media, and Internet of Things services, enterprise risk management has shifted its primary emphasis to cyber security. Better cybersecurity leads to increased consumer trust and income potential, but requirements for data protection and privacy are continually growing, making it more difficult to manage cybersecurity (Lee, 2021). One of the strategies for managing the risks associated with cyber security is limiting data access. This is done to avoid putting sensitive information at risk. Cybersecurity refers to a collection of technologies, processes, practices, and response and mitigation measures that are designed to protect networks, computers, programs, and data from being compromised, damaged, or inappropriately accessed. It also aims to maintain the confidentiality, integrity, and availability of this information (Panda & Bower, 2020).

In today's increasingly digital world, the importance of maintaining strong cyber security can be attributed to a number of factors, including the following: Cyberattacks can be extremely expensive for businesses; in addition to monetary losses, a data breach can result in irreparable damage to a company's reputation. In addition, cyberattacks are becoming increasingly damaging as time goes on. The methods that cybercriminals use to launch cyberattacks are becoming increasingly sophisticated as time goes on. As a result of regulations such as GDPR, companies are being put under increased pressure to improve the security of the personally identifiable information that they store. Because of the factors mentioned above, cyber security has emerged as an essential component of the company, and the primary focus now is on developing appropriate response plans that lessen the negative effects of cyberattacks, (Tariq, 2018).

One example of a cyberattack is a virus, which can infect multiple computers and spread throughout a network with the intention of causing damage to the targeted system. The worm is another type of computer virus. It is a self-replicating program that can be instructed to carry out a variety of functions, such as deleting files and sending documents via e-mail. Even while it is replicating itself, a worm can still have a negative impact on the traffic that is moving through a network. In addition, there is the so-called "Trojan horse," which is a malicious piece of software that takes the form of otherwise innocuous software. Discretionary environments are typically less secure and more prone to attacks by Trojan horses because security is user-focused and directed. As a consequence of this, the security of the whole environment may be at risk if just one user account is vulnerable to attack. The Logic Bomb is a form of malware that remains dormant until it is activated, which is the final type of cyber-attack. A logic bomb is an example of an asynchronous attack that can be used, (Tariq, 2018).

The report by Security Intelligence Solutions (2020) outlined the steps that must be taken in order for any company to evaluate the cybersecurity threats that they face. Among these is the Identify function, which entails developing an organizational understanding of the cybersecurity risk to systems, assets, data, and capabilities. Also included here is the Protect function. It is impossible to make effective use of the Framework without completing the tasks listed under the Identify Function. An organization is able to target and prioritize its activities in accordance with its risk management strategy and the business needs of the organization when it has a thorough understanding of the business context, the resources that support important functions, and the cybersecurity risks that go along with them. The second step, known as the protect function, involves organizations putting appropriate safeguards into place and putting them into operation in order to guarantee that essential infrastructure services are provided. The scope of any potential cybersecurity incident can be restricted or contained with the assistance of the Protect Function. A few examples of result categories that fall under this function's purview include access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology, (Wu et al., 2020).

There is also the detect function, which entails the creation and implementation of relevant operations in order to detect the emergence of a cybersecurity event. This function is similar to the monitor function in that it monitors for any changes in the environment. Real-time event detection pertaining to cybersecurity is made possible by the Detect Function. Some examples of the results Categories that can be found within this Function include Security Continuous Monitoring, Anomalies and Events, and Detection Processes. A further phase is known as the reply function, and its responsibilities include the creation and execution of the appropriate activities to react to a detected cybersecurity event. The Respond Function provides support for the capacity to contain the impact of any potential cybersecurity event that may occur. The following are some examples of result categories that fall under the purview of this
function: response planning, communications, analysis, mitigation, and improvements. The final stage is called the recover function, and it entails planning and implementing necessary measures to maintain resilience plans and restore any capabilities or services that have been harmed as a result of a cybersecurity event. This function comes at the end of the process, after all other stages have been completed. The Recover Function facilitates a speedy return to normal business operations in order to reduce the disruption caused by a cybersecurity incident. This function can produce a variety of results, some of which include the following: recovery planning, improvements, and communications, (Wu et al., 2020).

It is critical to implement the risk management practices for cybersecurity. On the other hand, there are circumstances in which they are not sufficient. Threats to a company's cybersecurity do exist, and businesses can and do fall prey to them. It's common for incident response plans to consist of nothing more than a contact person, which is inefficient. Techniques for the management of cybersecurity risks need to be consistently implemented in order for them to be effective.

Cyber-attacks have now become an unavoidable digital risk that even the most sophisticated financial institutions will never be able to completely eliminate cyber threats, no matter how much money they invest in cutting-edge protection technologies (Hausken, 2020). When a cyber-attack jeopardizes data availability, confidentiality, or integrity, it can trigger fear and cascading repercussions, resulting in poor insurance security performance. This will have an impact on stakeholders, so the insurance industry should adopt cybersecurity management techniques to address the issue of cyber-attacks. The purpose of this study was to determine the impact of cybersecurity risk management strategies on the insurance industry's performance.

Theoretical and Conceptual Background

Hollnagel's Theory of Resilience

According to the theory of resilience that was proposed by Hollnagel (2017), resilient performance denotes that an organization is able to continue its required operations in both predicted and unforeseen conditions by modifying its activities prior to, during, and after particular events.

According to Hollnagel (2017), in order for businesses to achieve resilient performance, they need to develop four capabilities: the ability to anticipate, monitor, respond to, and learn from their experiences. The ability to see what will take place in the future is referred to as the ability to anticipate. Examples of this include the possibility of disruptions, the introduction of new requirements or limits, or the introduction of innovative opportunities. The capability to monitor takes into account how well an organization can recognize shifts in working conditions, in addition to the indicators that are utilized to keep track of what's going on both inside and outside the building. To have the capability to respond, one must be aware of what actions to take and be able to execute those actions in a prompt and effective manner in response to events. This includes adapting to changes, disruptions, and opportunities that occur both regularly and irregularly by carrying out activities that have been pre-planned, modifying existing methods of labor, and/or devising new modes of operation (Chuang et al., 2020). In conclusion, having the capacity to learn requires having an awareness of what has happened as well as the ability to apply what has been learned.

Notably, Hollnagel (2017) acknowledges that cultivating the four potentials does not necessarily imply resilient performance when it is required, such as during a crisis. This is an important point to make. It is more likely for a company that has built them to execute in a resilient manner than it is for a company that has not built them, according to him. He continues by stating that an organization will be unable to maintain performance if there are no potentials to be found anywhere in the entire entity. This idea serves as the foundation for our research because it incorporates strategies for the management of cybersecurity risk that, when carried out in an efficient manner, can assist an organization in achieving resilient performance.

Empirical Review

Abdulrahim (2019) carried out a research study on the topic of managing cybersecurity as a business risk in small and medium-sized enterprises that are focused on information technology. The purpose of this research was to identify the most significant cybersecurity threats that Kenyan small and medium-sized enterprises (SMEs) are currently facing and to devise an implementation strategy that will provide a road map for the management of cyber-risk as a business risk. Case studies were used in the research. It centered on gaining a comprehensive understanding of the cybersecurity risk management practices utilized by the designated SME. Research that was conducted included both quantitative and qualitative methods. In order to perform an analysis on the obtained quantitative data, it was first given a numerical classification. In order to make analysis easier, the qualitative data that was gathered from primary sources was arranged in a methodical fashion. The findings of the research indicate that cybersecurity investments, cybersecurity management, training and awareness, cybersecurity policy programs, cybersecurity vulnerability management programs, real-time network monitoring, and incident management all play a significant role in the management of cyber-risk within SMEs. For the purpose of assisting in the management of cyber-risk, the implementation strategy that was developed offers a road map with proposed timelines. The research showed that the NIST cybersecurity framework is applicable to the environment of small and medium-sized enterprises (SME). This cybersecurity strategic plan was developed outlining an implementation roadmap to improve the cybersecurity posture of the organization based on the gaps identified within the environment and supplemented by a literature review. This plan was developed based on the findings of the environmental scan as well as the findings of the literature review.
Cyber resiliency

Kasanga, (2021) conducted research on the outcomes of various strategies utilized by commercial banks in Kenya for the purpose of enhancing their cyber resiliency. This study was carried out with the intention of determining the extent to which various cyber resilience techniques have an influence on the level of cyber resiliency present in Kenyan commercial banks. We used an explanatory research design, and our target population consisted of 39 department heads working in commercial banks in Kenya. Cybercrime was the topic of our investigation. In addition, a census methodology was utilized in the research, and as a result, all of the directors of cybercrime departments at Kenyan commercial banks participated in the investigation. This researcher made use of both primary and secondary sources of information. The secondary data obtained from the annual reports of Kenyan commercial banks were compiled using a data collection sheet that was used to collect the data. In order to collect information from employees working in information and communication technology, cyber security, operations, and risk departments, the study utilized semi-structured questionnaires.

The generation of both qualitative and quantitative data was accomplished through the use of a semi-structured questionnaire. According to the findings of the study, commercial banks in Kenya had implemented a significant amount of privilege restriction, coordinated protection, dynamic positioning, substantiated integrity, analytical monitoring, and dynamic representation. Nevertheless, deception as a strategy for enhancing cyber resilience had only been implemented to a limited extent. In addition, the research found that various approaches to cyber resilience, such as analytical monitoring, adaptive response, coordinated protection, dynamic representation, dynamic positioning, privilege restriction, and substantiated integrity, had a significant and favorable effect on cyber resilience in Kenyan commercial banks. In addition, the influence of deception on the cyber resiliency of commercial banks in Kenya is negligible. According to the findings of the study, Kenyan commercial banks should implement deception technology in order to make their enemies misdirect or waste their resources, delay the effect of an attack, confuse and mislead their opponents, and cause delay in the effect of the attack. In addition, commercial banks ought to utilize malware and forensic analysis in order to evaluate the actual damage caused by cyberattacks. Analytic monitoring ought to be utilized for the purpose of gathering, analyzing, and utilizing data in order to identify vulnerabilities.

Effective financial risk management

Mwaura, (2020) conducted a study with the intention of determining the extent to which effective financial risk management contributes to the high financial performance of SACCOs in Nairobi City County. The study opted to use a descriptive research design for its methodology. Since Nairobi City County is the county with the highest physical concentration of Savings and Credit Cooperative Societies, the population that was targeted included all 41 of these cooperatives in order to obtain comprehensive information. This was done because Nairobi City County is the county with the highest population density. Since a census survey was utilized, each of the 41 Savings and Credit Cooperative Societies was included in the sample. In order to collect the necessary information, we visited the website of the SASRA and downloaded the annual financial reports submitted by the Savings and Credit Cooperative Societies located within Nairobi City County between the years 2014 and 2018. In order to ensure that the data collected was accurate, secondary figures were acquired. This is because conducting research successfully requires collecting data in an accurate and methodical manner. The findings of the study indicated that there was a discernible connection between the effective management of financial risks and the superior financial performance of SACCOs. According to the findings of the research, Savings and Credit Cooperative Societies would benefit from increasing their use of financial risks management in their business operations. This is due to the fact that it was discovered that the use of financial risks management has a positive impact on the financial performance of Savings and Credit Cooperative Societies.

A study was carried out by Osiero (2016) to investigate the effects of risk management practices on the financial performance of non-life insurance companies operating in Kisii County, Kenya. This study's objective was to investigate the effects of risk management procedures on the financial performance of non-life insurance companies that were active in Kisii County, Kenya. In order to collect data, a descriptive survey research design was carried out. The target population consisted of 237 individuals, including 116 directors and 121 senior managers who were actively involved in the risk management of ten different insurance companies. The method used to get the sample was stratified random sampling, and the sample size was forty-eight respondents. This number of respondents is equivalent to twenty percent of the target population.

A questionnaire of a certain format was used in order to collect the primary data. Secondary data was collected from published reports and financial statements that were presented to IRA during the five-year period between 2010 and 2014. This data was then analyzed with descriptive and inferential statistics, and the results were presented with frequency tables, percentages, charts, and regression analysis. Based on findings on the extent to which effects of risk identification practice affect financial performance, the study concludes that an increased number of people understand the importance of insurance. Based on findings on the extent to which effects of risk mitigation practice affect financial performance, the study concludes that risk can never be eliminated completely. Both of these findings are based on the findings on the extent to which effects of risk mitigation practice affect financial performance. The study recommends that insurance companies adopt appropriate product pricing in line with estimated risk, which will ultimately increase profitability. The study also recommends that insurance companies structure their products or set competitive premiums to curb competition faced from rivalries and therefore avoid losing customers to the competitors.
A study on the impact of financial risk on the financial performance of deposit taking savings and credit co-operatives in Kenya was carried out by Gweyi (2018). This research was conducted with the intention of determining the extent to which financial risk affects the overall financial performance of deposit-taking savings and credit co-operatives in Kenya. In particular, the purpose of the study was to analyze the impact on financial performance of deposit taking savings and credit co-operatives in Kenya of credit risk, liquidity risk, interest rate risk, operational risk, and the moderating effect of firm size of the DT Sacco. The research design used in this study was a descriptive one. For the purpose of this study, the population of interest consisted of 164 Sacco societies that accepted deposits and were authorized to conduct deposit-taking Sacco business in Kenya for the fiscal year that ended in December 2016. Census data were utilized for the study, and all DT Saccos were taken into consideration. STATA Version 13 was used to collect and analyze data from a balanced panel consisting of 135 deposit-taking Saccos over the course of six years, from 2010 to 2015. This data represented an 82.32 percent success rate. The analysis of the data included both descriptive and inferential statistical methods. According to the findings, the four variables of credit risk, liquidity risk, interest rate risk, and operational risk all have a significant and negative impact on the organization's overall financial performance. The relationship between financial risk and financial performance of deposit-taking Saccos in Kenya is moderated by the size of the firm, which has an effect on the strength of the relationship. They need to know how credit policy affects the operation of their DT Saccos to ensure judicious utilization of deposits and maximize profit; DT Saccos should manage liquidity risk by reinforcing its own resources since depositors could at any time and for unexpected reasons, withdraw their deposits to seek investment elsewhere. The study gives recommendations, some of which include setting up a clear credit policy that will not negatively affect profitability. In addition, they need to know how credit policy affects the operation of their DT Saccos.

**Cyber fraud and the risks**

Jegede and Olowookere (2016) carried out research on the prevalence of cyber fraud and the risks it poses to business environments in Nigeria. The participants of the study were the various financial institutions that are located in Nigeria. According to the findings, detected risks need to be properly addressed in order to prevent secondary impacts that lead to vulnerabilities that interfere with the life of the institution as well as the well-being of its customers. Institutions have an additional responsibility beyond the installation of threat response technologies: they must work to strengthen the trust environment. They have a responsibility to their customers to keep them informed about the existence of actual and potential risks posed by the online environment. In order to avoid the compromise of personal information that is vital to the clients' financial and domestic survival, protective actions need to be implemented, and obtaining clients' consent is essential in this regard, particularly when such requests are made for secondary uses of the information.

Opondo (2021) carried out a research study in Kenya to investigate the risk management strategies and performance of projects carried out by the national irrigation board. The research utilized a descriptive research design, and the data collection involved both face-to-face interviews and the distribution of structured questionnaires. At the time of this survey, the Kenyan National Irrigation Board had a total of 250 project managers working on the implementation and management of its numerous irrigation programs and schemes. The researcher took a sample size of 135 from this population and selected participants using both stratified and simple random sampling techniques. As a result, the researcher was able to obtain a response rate of 71.11 percent. We used both descriptive and inferential statistics to make sense of the data we gathered from the respondents. The findings that were obtained demonstrated that the management strategies of risk retention, risk reduction, risk avoidance, and risk transfer each have a significant implication and effect on the performance of the project. According to the findings of the study, one way for improvements to be made is for entities to establish funds that are designed to facilitate the retention of risks in the event that they actually occur.

Gatzert and Schubert, (2022) carried out a textual and empirical investigation into the management of cyber risk in the banking and insurance industries in the United States. In this paper, the authors begin by developing a cyber risk consciousness score by applying a text mining algorithm to the annual reports of large and mid-cap US financial institutions and insurers between the years 2011 and 2018. After that, they classify the companies' cyber risk management based on keywords in order to research the factors that determine value relevance. Their findings indicate that businesses across all sectors are becoming more aware of the dangers posed by cyberattacks. In addition, they find that across the entire sample, companies belonging to the banking industry that have a higher cyber risk consciousness score as well as a higher general risk awareness are more likely to implement cyber risk management. This is true for both industries taken separately as well. They find the opposite to be true in the case of profitable companies across the board and in the insurer subsample specifically. Finally, they find that there is a significant positive relationship between cyber risk management and firm value as measured by Tobin's Q for the entire sample as well as the subsamples of banks and insurers. This relationship holds true across all three groups.

**Conclusions**

The study adopted a desktop methodology. Desk research refers to secondary data or that which can be collected without fieldwork. Desk research is basically involved in collecting data from existing resources hence it is often considered a low-cost technique as compared to field research, as the main cost is involved in executive’s time, telephone charges and directories. Thus, the study relied on already published studies, reports and statistics. This secondary data was easily accessed through the online journals and library.

The results were grouped into various research gap categories namely as knowledge and methodological gaps:

338
According to the findings, detected cyber risks should be addressed properly in order to avoid secondary impacts that lead to vulnerabilities interfering with the lives of insurance institutions and their customers. Additionally, institutions need to work to build a more trusting environment. Customers expect them to keep them informed about any and all risks associated with using the internet. As a result, safeguards must be put in place to prevent the loss of personal information that is critical to a client's financial and domestic well-being. Cybersecurity risk management practices have a positive impact on insurance sector performance, according to the study.

Since it has been found that cybersecurity risk management strategies have a positive and significant impact on the performance of the insurance sector, the research recommends that insurance companies increase their use. Additionally, financial institutions ought to have funds set aside specifically for the purpose of facilitating the retention of risks, in the event that these risks actually materialize. In addition, the research suggests that insurance companies reorganize their product lines or establish premiums that are competitive in order to reduce the threat posed by their rivals and, as a result, prevent the loss of customers to those rivals. The research further suggest that insurance companies adopt appropriate product pricing in line with estimated risk, as this will ultimately lead to increased profitability.

Acknowledgement

Author Contributions: Conceptualization, Methodology, Writing—Original Draft Preparation, Writing—Review And Editing, by author. Author has read and agreed to the published the final version of the manuscript.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to that the research does not deal with vulnerable groups or sensitive issues.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to privacy.

Conflicts of Interest: The authors declare no conflict of interest.

References


