INTERNATIONAL JOURNAL OF STRATEGIC MANAGEMENT

International Journal of Strategic Management
ISSN: 2314-2896
Volume 4, Issue 2, pg. 407-420, 2021

EFFECT OF RISK MANAGEMENT STRATEGIES ON SUPPLY CHAIN PERFORMANCE OF CYBERSECURITY FIRMS IN KENYA

[1] Munene Hellen Muthoni, [2] Karungani Walter (PhD)
[1]Master Student, Jomo Kenyatta University of Agriculture and Technology
[2]Lecturer, Jomo Kenyatta University of Agriculture and Technology

ABSTRACT

Risk management strategies have significantly influenced cybersecurity supply chain. The findings of a study on risk management strategies and supply chain performance by Boone (2017) empirically established that the global cost of cybercrime is likely to increase to $6 trillion by 2021. Deloitte Kenya (2018) pointed out that more than 35 percent of businesses in Kenya have implemented automated systems and techniques. Consequently, increase in technology leads to increase in cyber criminals. According to Qazi, Quigley, Dickson & Ekici (2017) risk management strategies enhance long term growth of cybersecurity firms through secure productive relationship with its stakeholders. This study, therefore, will focus on determining effect of risk management strategies on supply chain performance of cybersecurity firms in Kenya. The study will be limited to the following objectives: To assess the effect of risk avoidance on supply chain performance of cybersecurity firms in Kenya; To determine the effect of risk transfer on supply chain performance of cybersecurity firms in Kenya; To find out the effect of Risk Reduction on supply chain performance of cybersecurity firms in Kenya and to assess the effect of risk acceptance on supply chain performance of cybersecurity firms in Kenya. This study will adopt cross-sectional survey. The target population will be 571 respondents who will comprise of the professional employees working at the top, middle and operational levels of management of cybersecurity firms in Kenya. Stratified random sampling technique will be used to determine the specific sample size of each strata of the study. Data will be obtained through questionnaire. Data analysis will be done through SPSS Version 24 and the analyzed data will presented in form of tables. The study will aim to provide improvement and recommendations to existing literature and further recommend areas for future study to the cyber security firms, the National Government and County Governments on how to ensure successful and effective implementation of risk management strategies.

INTRODUCTION

Risk has always been part of the supply chain. It is a reality inside and outside the four walls of any organization (Wiengarten, Humphreys, Gimenez, McIvor, 2016). It is no surprise then that as Enterprise Risk Management (ERM) programs proliferate, they have naturally begun to address anticipated and unanticipated events occurring both upstream and downstream in the supply chain. Upstream of an organization are the suppliers who create goods and services used in a company's own operations (Fan, Li, Sun, & Cheng, 2017). These include raw components or materials that flow into direct manufacturing as raw materials. There are also indirect products and services that facilitate the company's actual operations. The downstream supply chain efficiently distributes a company's products or services to its customers. All contracted suppliers, both upstream and downstream, must be proactively managed to minimize financial, confidentiality, operational, reputational, and legal risks (Fan & Stevenson, 2018).

It is worth noting that the challenge of risk management strategies along the supply-chain has been exacerbated by globalization, where even sensitive products like defense systems use raw materials, circuit boards, and related components that may have originated in countries where the system manufacturer did not even know it had a supply chain (Kiani Mavi, Goh, & Kiani Mavi, 2016). This increased complexity has brought with it more potential failure points and higher levels of risk. Yet progress in addressing these risks has been slow. A recent example of the developing capability of cyber threats was observed in the food industry, where complacency led to the belief that IT-related risks would only affect office-based work (Khursheed et al., 2016). However, more elaborate malware goes beyond the boundaries of offices and can infect automated production systems and the wider supply chain network.

The global cost of cybercrime is likely to increase to $6 trillion by 2021(Giannakis & Papadopoulos, 2016). Cybercrime refers to all illegal activities carried out using technology. Cybercriminals who range from rogue individuals to organized crime groups to state-sponsored factions use techniques like phishing, social engineering, and all kinds of malware to pursue their nefarious plans. The costs associated with cybercrime varies from loss of data, money loss, decrease in the levels of productivity, unauthorized disclosure of personal data as well as financial data as well as reputational damage within an organization (Cybersecurity Ventures, 2017). According to Achuora (2017) the number of internet users will increase to 6 billion by the year 2022. Further, the users will have increased to 7.5 billion by the year 2030 (Cybersecurity Ventures, 2017).

According to a global risk survey conducted by various consultancy and insurance firms (e.g., Gartner, AXA, Society of actuaries, Deloitte) in 2018, cyber security and data breaches emerged as the top enterprise risk to organizations. Supply chains are the backbone of evolving technological ecosystems. Industry 4.0 concepts such as the Internet of Things, Additive Manufacturing, Virtual Reality, Artificial Intelligence, Blockchain, both reflect, expand, alter and innovate the relationships between supply chain partners (Qazi, Quigley, Dickson & Ekici, 2017). However, developments in cyber security responses lag these advances in the digitalization of supply chains. Boone (2017) asserts that supply chains have unintentionally expanded their vulnerability by imprudently collaborating with many diverse partners. For envisaging risks of extreme events in solving multiple problems of probabilistic nature, which cannot be encompassed by the traditional definition, methods have been developed such as partitioned multi objective risk analysis (Sotic, Pavlovic & Ivetic, 2015), which determine conditionally expected risk values.
According to Serianu (2016) studied on the challenges cybersecurity systems face in African. He established that countries lose at least $2 billion to cyber-attacks in every two years. In East Africa, Kenya recorded the highest losses with $171 million lost to cyber criminals. Tanzania lost $85 million while Ugandan companies have lost $35 million. Over one-third of organizations that experienced a breach in 2016 reported substantial customer, opportunity, and revenue loss of more than 20 percent, (Cisco. 2017). The Africa Cyber Security Report 2017 indicated that the region lost $394 million in 2019 to cyber criminals. Kenya consequently lost at least $210 million, closely followed by Tanzania losing $99 million and Uganda losing $85 million.

According to KnowBe4 (2019) South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius, and Botswana have found that people living on the continent are not prepared for the cyber threat. The study established that 65% of the respondents were concerned about cybercrime due to fear of unknown. From ransomware to phishing to malware and credential theft, users are not protecting themselves adequately because they mistakenly think they are informed, ready and prepared. The study further established that 55% believe organizations recognize a security incident. The researcher concluded that cybercrime should be cubed if the region is to encourage embracing information communication technologies.

In Kenya, the key factors contributing to disrupting supply chains is the focus on lean supply chains in academia and industry. Zero-inventory and just-in-time movement of goods became the dominant model that increased the sensitivity of supply chains (Ochieng, 2019). Little issues quickly become big issues. In addition, supply chains have become more modern and wider, increasing the order to delivery cycle times by a factor of four or five. This acts to amplify the potential of a disruption and the impact (Nyang'au, 2016). Outsourcing has also become the dominant model, increasing the forces driving disruptions such as other customers competing for volume and attention, information flow issues, mistrust, win-lose negotiations, financial stress, misalignment of interests and goals. These have increased the likelihood of a disruption exponentially (Mburu, 2017).

In 2018 Serianu estimated the cost of cybercrime in Kenya to be USD 175 million in 2016, an increase from the USD 150 million reported in 2015. In July 2019 Communications Authority revealed that Kenyan organizations were hit by about 11.2 million cyber threats, is a 10.1 percent increase in the number of incidences, in the first three months of 2019 when compared to the previous quarter. Further, based on Africa Cyber Security Report- Kenya released early 2019 by Serianu, about 60 percent of local companies are short of cybersecurity professionals.

The Kenya Information and Communications Act, 1998, mandates the Communications Authority of Kenya (CAK) to develop a national cyber security management framework. It is in this regard, and in order to mitigate cyber threats and foster a safer Kenyan cyberspace, that the government established the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC), a multi-agency collaboration framework which is responsible for the national coordination of cyber security as Kenya's national point of contact on cyber security matters. This in accordance with the provisions of the Kenya Information and Communications Act. The enactment of the Computer Misuse and Cyber Crimes Act of 2018 has gone a long way in strengthening this multi-agency collaboration framework, among other key facets that support national cyber security resilience.

The National KE-CIRT/CC coordinates response to cyber security matters at the national level in collaboration with relevant actors locally and internationally. The National KE-CIRT/CC is based at the CA Centre and comprises of staff from the Communications Authority and law enforcement agencies. The National KE-CIRT/CC detects, prevents, and responds to various cyber threats targeted at the country on a 24/7 basis, having commenced round-the-clock operations in 2017.The National KE-CIRT/CC therefore acts as the interface between local and international ICT services providers whose platforms are used to perpetrate cybercrimes, and our Judicial Law and Order Sector which investigates and prosecutes cybercrimes.

Statement of the problem

Risk management strategies have significantly influenced cybersecurity supply chain. The findings of a study on risk management strategies and supply chain performance by Boone (2017) empirically stablished that the global cost of cybercrime is likely to increase to $6 trillion by 2021. Deloitte Kenya (2018) pointed out that more than 35 percent of businesses in Kenya have implemented automated systems and techniques. Consequently, increase in technology leads to increase in cyber criminals. According to Qazi, Quigley, Dickson & Ekici (2017) risk management strategies enhance long term growth of cybersecurity firms through secure productive relationship with its stakeholders.

Studies conducted by Khojasteh (2017) summarized that protecting your data, and the data of all your value chain partners, can be just as important as protecting your goods and your facilities. According to him, approximately 95.5 percent of the operations carried out in an organization are SCM activities hence across an organization, professionals must consider the implications of a data breach and plan accordingly. Manners-Bell, (2017) investigated the impact of various types of supply chain risk on supply chain performance. The findings show supply side risk and demand side risk as the only significant predictors of supply chain performance. Sayed & Sunjka, (2016) conducted a study on the relationship between supply chain risk management and performance of manufacturing firms in Kenya. In their empirical study, they concluded that supply chain disruptions can lead to a company's long-term negative financial performance. It is therefore obvious that companies may end up losing millions of dollars due to cost volatility, non-compliance fines, supply disruption, and incidents that cause damage to the reputation of the brand (Macharia, 2017; Serianu (2018) & Communications Authority of Kenya CAK, (2019)).

The findings of a study conducted by Macharia (2017) pointed out that 25 percent of cybersecurity firms in Kenya have successfully implemented risk management strategies and were willingly modifying supply chain practices to reduce threats, duplication and waste while facilitating improved performance, efficiency, and effectiveness. Serianu (2018) stated that the accumulated cost of cybercrime in Kenya rose to USD 175 million in 2016 from USD 150 million reported in 2015. Further to this the (CAK, 2019) revealed that Kenyan organizations had been hit by an additional total cost of approximately KSH. 11.2 million Cyber threats which represented 10.1 percent increase from the previously reported incidences. This represents 2.5 percent fall in gross domestic product (GDP). This study focused on effect of risk management strategies on supply chain performance of cybersecurity firms in Kenya. Therefore, the researcher connected the identified gap by assessing the effect of risk management strategies on supply chain performance of cybersecurity firms in Kenya.

Objectives

1. To assess the effect of risk avoidance on supply chain performance of cybersecurity firms in Kenya
2. To determine the effect of risk transfer on supply chain performance of cybersecurity firms in Kenya.

International Journal of Strategic Management
ISSN: 2314-2896
Volume 4, Issue 2, pg. 407-420, 2021

LITERATURE REVIEW

Theoretical Framework

Dynamic Capability Theory

Dynamic capability theory emerged from Gary Hamel's working paper 1989 "multinational strategy research leading to Core Competencies of the Corporation". This theory emphasizes the ability of a firm to blend, construct, and figure again internal and external capabilities and speak on the swift evolving environment. Ever-changing competences therefore mirror the firm's capacity to attain new and inventive types of competitive vantage point, given dependencies of path, and positioning of markets (Helfat et al., 2007 & Teece, 1997). Companies with supply chains must deal with factors related to increased competition. These competition-related factors make forecasting demand and adjustment to unexpected product life cycle and customer preferences a huge challenge.

Risk avoidance is the most effective risk management strategy in that by avoiding an activity, any chance of loss is eliminated (Khan & Burnes, 2007; Tuncel & Alpan, 2010). Avoidance strategies are classified as Type 1 and Type 2 (Manuj & Mentzer, 2008). Type 1 avoidance strategy is used when the risks associated with operating in each product or geographical market, or working with suppliers or customers, is considered unacceptable. Manuj and Mentzer (2008) suggested that avoidance takes the form of exiting through divestment of specialized assets, delay of entry into a market or market segment, or participating only in low uncertainty markets. This type of strategy is aimed at reducing chances of risk occurrence to zero by ensuring that the risk does not exist (Manuj & Mentzer, 2008).

Resource dependence theory

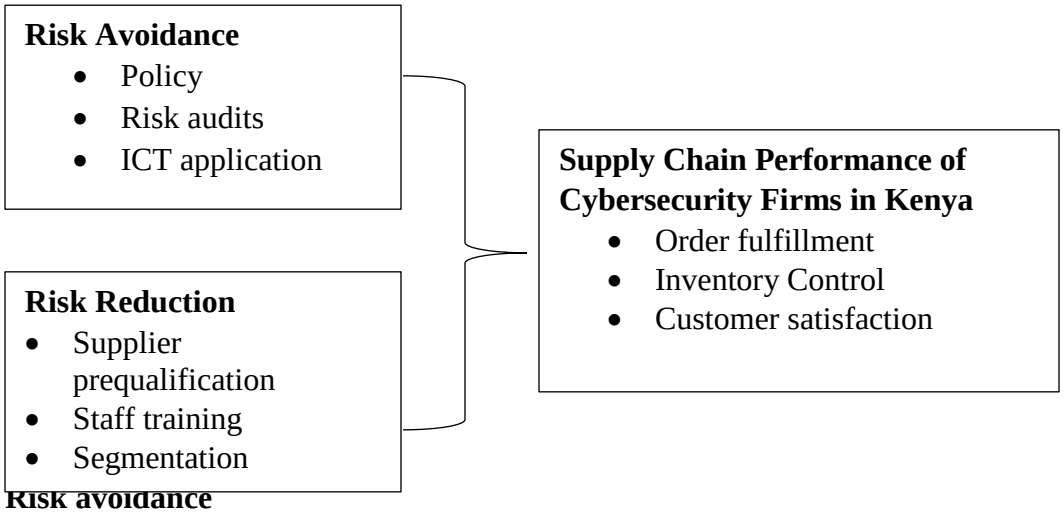
Although it had already been known for some time that organizations rely on external resources, the theory on the dangers of that reliance did not come into prominence until the 1970s. Authors Jeffrey Pfeffer and Gerald R. Salancik published the book, 'The External Control of Organizations: A Resource Dependence Perspective (Pfeffer & Salancik, 1978). In it they discussed where power and dependency come from, and how organizations can use this power to manage dependent organisations. Managers and leaders are always looking for advantages to strengthen their relationships towards other organisations and to strengthen and improve their own organisations. The Resource Dependence Theory (RDT) is based on the principle that resources are the key to an organisation's success and that access to and control over these resources are a foundation for power (Hillman, Withers & Collins, 2009). Resource Dependence Theory (RDT) came out of a study into how organisations' external resources affect the behaviour of those organisations. In other words, the theory examines the relationship between organisations and the products they need to operate. Resources come in many forms, such as raw materials, financing, and employees. Acquiring these external resources is an important aspect of the strategic and tactical management for any business (Hillman, Withers & Collins, 2009).

In order to prevent such dependencies, organisations often develop strategies and internal structures that have been designed to give them a better negotiating position when it comes to resource-related transactions. These activities include: Political action, increasing scale of

International Journal of Strategic Management
ISSN: 2314-2896
Volume 4, Issue 2, pg. 407-420, 2021

production, Diversification and developing new relationships with other organisations. Particularly diversification of product or service lines can reduce the dependency of businesses and increase their power and leverage.

Conceptual Framework



Risk avoidance

The risk prevention strategy involves eliminating risk by withdrawing from the risk situation (Ivanov, et al., 2019). In other words, it is designed to set the probability of the risk event to zero by removing the source of the risk. This allows purchasing managers to avoid supplier sustainability risk by running out of the owner risk provider and switching to an alternative supplier with a relatively clean sustainability balance. In June 2013, Wilmar International Ltd., the world's largest palm oil trader, decided to cut ties with all Indonesian suppliers that could eliminate farmland with illegal fires (Yun, Pakiam & Listiyorini, 2016).

A cybersecurity program is defined by its underlying policy. The company's security policy is the articulation of the objectives of the organization agreed by the administration, which define the requirements to be followed (Ivanov, et al., 2019). Instead of guidelines, the Directive establishes binding behaviour. The creation of a security policy requires management to express what it deems necessary and what risks they are willing to accept (Chepleting & Musau, 2019). Rather than simply outsourcing a security model, the best practice is to engage the company's leadership in an educational process about security risks in order to develop an informed consensus between and with strong leadership, the authority to develop and adhere to the cybersecurity strategy. Unlike cybersecurity policy, security policy is a term deliberately used (Haj Mohammad & Vachon, 2016). Security includes physical security, personnel security, cybersecurity, and support for business continuity procedures.

Risk Reduction

Cyber security threat mitigation refers to policies and processes put in place by companies to help prevent security incidents and data breaches as well as limit the extent of damage when security attacks do happen (Stroud, 2017). Monitoring-based Risk Reduction strategy focuses on assessing the processes or actual performance of suppliers against specific characteristics or

performance criteria to verify their compliance with the requirements (Jiang, 2019). As part of this approach, buyers usually conduct supplier prequalification; collect and process suppliers' information, set proper criteria, assess the sustainability-related aspects of incoming goods and the suppliers that provide them through surveys and audits, and ask the suppliers to report on different dimensions of their social and ecological performance (Bowen, Cousins, Lamming & Farukt, 2017; Seuring & Müller, 2018). These are usually enforced through written social/ecological requirements within contracts (Ciliberti, Pontrandolfo & Scozzi, 2018; Neef, 2016), requiring third-party certifications (Morali & Searcy, 2017), and/or imposing the buyer's code of conduct on the suppliers (Andersen & Skjoett-Larsen, 2019).

The purpose of staff training is to raise basic awareness of risk management concepts and mechanisms, to enable participants to identify and manage risks in their own units and to strengthen project management through adequate forward planning of potential risks (Morali & Searcy, 2015). Risk management training can help your team to recognize and understand how managing their risk benefits them, their performance, and the broader enterprise Seuring & Müller, 2018). Only then can they make precise and powerful decisions on behalf of your business, driving actions that work in the real world. According to Jiang (2019) the major goal of risk management training is to teach staff members "how" to carry out the risk management procedures as described in the Risk Management Policies and Procedures Manual (RMPPM).

Empirical review

Study that was conducted by Manuj & Mentzer (2008) focused on the relationship between risk management and risk management strategies in supply chains. The study was a review of empirical literature supplemented with a focus group discussion and detailed interviews. The risk management strategies that the study focused on included speculation, security, hedging, postponement, control, and avoidance. The study established that risk avoidance was widely used and was highly effective. The methods of risk avoidance were delay of entry into markets deemed as high risk, divestiture of specialized assets, participating only in low-risk markets and forestalling adverse events.

Manuj & Mentzer (2008) found that risk avoidance strategies contributed to performance, other studied such as that by Sarkisyan, Casu, Clare, & Thomas (2009) established that risk management by securitization did not affect the performance of commercial banks.

In a study conducted by Sarkisyan, Casu, Clare, & Thomas (2009) the aim was to evaluate whether banks improve their performance when they securitize their debt. The study was conducted on commercial banks in the USA using data from 2001 to 2008. The study used a propensity score matching approach. The study established that securitization did not improve the performance of commercial banks.

Another study conducted by Chang, Ho, & Hsiao (2010) sought to determine how hedging affected risk exposure of commercial banks and how hedging affected financial performance. The study was conducted on European banks operating in 25 countries. The study established that banks that used more hedging were more exposed to risk. Data were obtained from banks' balance sheet and income statements retrieved from the Bank scope database. Analysis was conducted by linear regression. The study established that banks with high-risk exposure and

higher value used derivatives. This indicates that risk management through hedging affected performance as measured by firm value.

A study conducted by Mercieca, Schaeck, & Wolfe (2006) investigated how diversification affected the creditworthiness and earnings of low-level European credit companies. The study was conducted using data from 755 small banks in 15 countries. The study covered the time between 1997 and 2003. The Herfindahl Hirschman Index was used as a measure of diversification. Earnings were measured by Return on Assets (ROA) and Return on Equity (ROE). Z scores were used to conduct the analysis. The results suggested that diversification did not affect the profitability of small banks.

RESEARCH METHODOLOGY

This study adopted descriptive research design. According to Mugenda and Mugenda (2008) and Creswell (2003). Target population includes the individuals to be studied (Mugenda & Mugenda, 2003). The target population was 571 respondents who comprised of the professional employees working at the top, middle and operational levels of management of the of Cybersecurity firms in Kenya. The sampling frame of the study consisted of 571 respondents selected from the top, middle and operational level of management. Stratified random sampling technique was used in this study. This is because stratified random sampling is an unbiased sampling method that involves grouping heterogeneous population into homogenous subsets and thereafter selecting within the individual subset to ensure representativeness (Mugenda and Mugenda, 2003). Primary data was collected by using questionnaires. The questionnaires comprised both open and closed ended questions. The questionnaire was administered through emails method to give respondents enough time to give well thought out responses. Quantitative data was coded and entered statistical packages for Social Scientists (SPSS Version 24) and was analysed using descriptive statistics while qualitative data will be analysed using content analysis.

RESEARCH FINDINGS AND DISCUSSIONS

Response Rate

Eighty-six questionnaires were sent to respondents working in the cyber security industry. Seventy seven of the eighty-six sent questionnaires were responded to, resulting in a 89.5% response rate for the study. According to Orodho (2009), Mugenda and Mugenda (2012), a response rate of 50% and above provides adequate data that can be inferred to represent the population. The questionnaires were distributed via email with several visits to the various companies to present the introduction from the university and to answer queries concerning the studies. Quantitative data obtained from the questionnaires were presented in tables, frequencies and percentages as shown hereafter.

Descriptive Statistics

Effect of risk avoidance on supply chain performance of cybersecurity firms in Kenya

The study sought to determine the effect of risk avoidance strategies on the supply chain performance of cyber security firms. The respondents were required to respond based on their organization's practices as displayed in Table 1

International Journal of Strategic Management
ISSN: 2314-2896
Volume 4, Issue 2, pg. 407-420, 2021

Table 1 Descriptive Statistics for Risk Avoidance Strategies

Statements	Mean	Std. Deviation
Policy formation and implementation	4.6000	.54772
Risk audits hedges against unforeseen risky ventures.	4.6000	.54772
ICT application and adoption improves an organizations risk avoidance preparedness	3.2000	1.09545
Our organization practices risk avoidance to ensure order fulfillment, customer satisfaction and inventory control	3.200	.44721

N=77

Table 1 presents that majority of the respondents strongly agreed that policy formation and implementation is an effective way of risk avoidance for cybersecurity firms. This can be qualified by the mean=4.600 with a standard deviation from the mean of .54772. The study also established that many of the respondents strongly saw risk audits as an applicable measure to hedge against unforeseen risky ventures (mean=4.600, standard deviation=.54772). Concerning risk avoidance preparation, the respondents agreed that the adoption of ICT applications (mean=3.2000, standard deviation of 1.09545). The respondents also equally agreed that their respective organizations practice risk avoidance to ensure order fulfillment, customer satisfaction and inventory control with a mean of 3.2000 with a standard deviation from the mean of .44721.

Statements	Mean	Std. Deviation
Review risk policy and regulations of the organization	3.8000	1.09545
Audit the risk environment of the organization	4.4000	1.34164
Insure risky ventures Introduce new technology to the organization	4.0000	1.22474

Table 2 Descriptive Statistics for Risk Avoidance Strategies in Cyber Security Firms

N=77

Table 4.4 shows how often the respective organizations of the respondents practices the stated risk avoidance strategies. The respondents were of the opinion that they very often observed the review of risk policy and regulations within their organization as a practiced measure for risk avoidance (mean= 3.8000, standard deviation= 1.09545). The study also established that the respondents very often saw audits of risks in the environment by their organizations (mean=4.4000, standard deviation= 1.34164). Finally, this descriptive analysis of practiced risk avoidance strategies revealed that insurance of risky ventures and introduction of new technologies was a frequent risk avoidance practice in the respective cyber security firms.

Effect of Risk Reduction on supply chain performance of cybersecurity firms in Kenya

The study also wanted to investigate the effect of Risk Reduction strategies on the supply chain performance of cyber security firms in Kenya. Table 4.5 presents the descriptive statistics of the investigation.

Table 3 Descriptive Statistics for Risk Reduction Strategies

Statements	Mean	Std. Deviation
Supplier prequalification process introduces qualified vendors who assist in mitigating risks.	4.0000	.00000
Staff training boosts employee confidence and market know how on mitigating risks.	4.2000	.44721
Portfolio and market segmentation ensures businesses choose and venture in less riskier opportunities	4.4000	.54772
Our organization practices Risk Reduction to ensure order fulfillment, customer satisfaction and inventory control	4.8000	.44721

N=77

The respondents all unanimously strongly agreed that supplier prequalification is an effective Risk Reduction strategy. The response can be deduced to be unanimous due to the 0.0000 standard deviation from the mean, a clear indication that all the respondents opted to strongly agree with the statement. In line with the Risk Reduction objective, the study also required the respondents to comment on staff training which resulted in employee confidence and market know how. The majority strongly agreed the aforementioned was a great Risk Reduction strategy with a mean of 4.2000 and standard deviation= .44721. Portfolio and market segmentation was another Risk Reduction strategy that the research examined. It was found that many of the respondents highly agreed with the statement (mean=4.4000, standard deviation= .54772). Finally, the respondents were asked to give their observation if their organization's practice of Risk Reduction ensures order fulfillment, customer satisfaction and inventory control was effective. Majority of them strongly agreed with the statement with a standard deviation of 0.44721 from the mean.

Table 4 Descriptive Statistics for Risk Reduction Strategies in Cyber Security Firms

Statements	Mean	Std. Deviation
Prequalify the venders that do business with the organization	4.0000	1.73205
Train its staff on market emerging trends and needs	4.0000	1.73205
Market analysis and segmentation	4.6000	.54772

N=77

The above table 4.6 shows the results of observation of the frequency of the application of the stated Risk Reduction strategies in cyber security firms in Kenya. The respondents claimed that they often observed prequalification of venders in their respective firms (mean= 4.0000, standard deviation= 1.73205). The respondents also stated that staff training on emerging trends and needs coupled with market analysis and segmentation were frequently practiced within their firms as

Risk Reduction strategies with (mean=4.0000, standard deviation= 1.73205) and (mean= 4.6000, standard deviation =.54772) respectively.

Correlational Analysis

		Risk avoidance	Risk Reduction	Risk transfer	Risk acceptance
y variable	Pearson Correlation	.958*	.405	.700	.958*
	Sig. (2-tailed)	.010	.498	.188	.010
	N	77	77	77	77

The findings as presented in Table 4.12 reveal a positive and statistically significant association between risk avoidance as a strategy of improving supply chain performance of cyber security firms in Kenya. The researcher determined that a positive relationship where r=0.958 between risk avoidance strategies and supply chain performance at 5% significance level (p=0.000, <0.05). The association between Risk Reduction and risk transfer with supply chain performance in cyber security firms was found to be positive but statistically insignificant. The results from the Pearson correlation analysis also showed a positive and statistically significant association between risk acceptance as a strategy of improving supply chain performance of Cyber Security firms in Kenya. The analysis revealed a positive relationship where r=.958 at l (p=0.000, <0.05). Based on correlational analysis, risk acceptance and risk avoidance are the only variables with a statistically significant association with supply chain performance of Cyber Security Firms in Kenya.

Regression Analysis

The study conducted multiple linear regression analysis to determine the change in supply chain performance that can be explained by the risk management strategies: risk avoidance, Risk Reduction, risk transfer and risk acceptance.

Table 6 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.958	.918	.891	.001

The model summary Table 4.13 gives the coefficient of determination (R^2) is used to measure the extent to which the regression model explains the changes in the independent variables. R is the correlation coefficient which shows the relationship between the dependent and independent variables. The findings shows that there exists strong positive relationship between the independent variables and dependent variable as shown by R value (0.958). The coefficient of determination should have a value between zero and one (Robinson, 2010). As per the model of the study, R^2 = 0.918 which means that the independent variables, risk management strategies can contribute upto 91.8% in supply chain performance of Cyber Security Firms in Kenya while the remaining 8.2% can only be accounted for by other variables which have not been captured

in the study. The standard error has a value of 0.001 making the model more reliable. The model is a good fit because R squared value explains the y variable by more than 60%.

Table 4:15 Coefficients of Determination

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.
	B	Std. Error	Beta		
(Constant)	3.000	1.001		3.0764	.000
Risk avoidance X1	.564	.103	.472	.374	.000
Risk Reduction X2	.202	.078	.461	.197	.000

The analysis shows that 1% change in risk avoidance can contribute to 56.4% of the change in supply chain performance. A 1% change in risk reduction can contribute to 20.2% of the change in supply chain performance. Furthermore, 1% change in risk transfer strategies can contribute to 20% of the change in supply chain performance. A 1% change in risk acceptance strategies can contribute to 54.5% of the changes in supply chain performance. All these changes apply while holding all other factors constant. Therefore, these findings indicate that risk avoidance and risk acceptance strategies hold a lot of significance in the improvement of supply chain performance in Cyber Security Firms in Kenya.

SUMMARY, CONCLUSION AND RECOMMENDATION

Conclusion

Following the results of the study, it is worthwhile to conclude that there is a positive relationship between risk management strategies and supply chain performance of the cyber security industry in Kenya. Through risk avoidance, risk transfer, risk reduction and risk acceptance, cyber security firms in Kenya have been able to realize order fulfillment, inventory control and customer satisfaction performance. This is further explained per variable of the study as follows.

The study establishes that there is a positive relationship between risk avoidance and the supply chain performance of the cyber security firms in Kenya. The study further established that Policy formulation and implementation, carrying out risk audits, and ICT application are among the risk avoidance factors that affect supply chain performance of organizations as it was observed in the cyber security firms in Kenya. Therefore, the study concludes that cyber security firms in Kenya experience significant increase in the level of order fulfillment, inventory control and customer satisfaction when they embrace risk avoidance.

The results of the study have revealed that risk transfer has a positive influence on the supply chain performance of cyber security firms in Kenya. The study further established that outsourcing, entering indemnified contracts with suppliers, insurance of risks is among the risk transfer factors that affect supply chain performance of organizations as it was observed in the cyber security firms in Kenya. Therefore, following the results of the study, it is worthwhile to conclude that organizations supply chain performance is dependent on risk transfer.

Recommendations

Adopting a risk avoidance strategy means seeking to eliminate risk by withdrawing or not becoming involved in a high-risk activity (Chepleting & Musau, 2019). Organizations have the option to refrain from activities that carry unacceptable risks. However, on the other hand, a practitioner cannot use avoidance in all cases. The main disadvantage of this strategy is it is limiting a business's potential (Mtega et al. 2013). It is important to note that managing risk in this way, risk avoidance means not performing that activity that causes the risk. While some organizations are more risk-loving others are more risk-averse, thus this study recommends that organizations should establish a tipping point at which things become just too risky and not worth attempting (Yun, et. al., 2016).Risk transfer is an action or strategy that contractually shifts the risk of doing business from one party to another (Muteti, 2016). The purpose of risk transfer is to pass the financial liability of risks, like legal expenses, damages awarded and repair costs, to the party who should be responsible should an accident or injury occur on the business's property. Risk transfers can be outsourced, moved to an insurance agency, or given to a new entity as is what happens when leasing property (Kelman, 2016). Many liability losses occur through the transfer of risk, making it necessary for a Risk Control Consultant to assess the hazards and controls that could arise from various contracts and agreements. This is similar to other risk management and loss control efforts, such as assessing the workplace for potential hazards that could result in injury to an employee (Hillson, 2018).

REFERENCE

Agigi, A., Niemann, W., & Kotzé, T. (2016). Supply chain design approaches for supply chain resilience: a qualitative study of South African fastmoving consumer goods grocery manufacturers. Journal of Transport and Supply Chain Management, 10(1), 1-15.

Ahi, P., & Searcy, C. (2015). An analysis of metrics used to measure performance in green and sustainable supply chains. Journal of Cleaner Production, 86, 360-377.

Ambulkar, S., Blackhurst, J. V., & Cantor, D. E. (2016). Supply chain Risk Reduction competency: an individual-level knowledge-based perspective. International Journal of Production Research, 54(5), 1398-1411.

Aqlan, F., & Lam, S. S. (2015). A fuzzy-based integrated framework for supply chain risk assessment. International Journal of Production Economics, 161, 54-63.

Aqlan, F., & Lam, S. S. (2015). Supply chain risk modelling and mitigation. International Journal of Production Research, 53(18), 5640-5656.

Bak, O. (2018). Supply chain risk management research agenda. Business Process Management Journal.

Bandaly, D., Satir, A., & Shanker, L. (2016). Impact of lead time variability in supply chain risk management. International Journal of Production Economics, 180, 88-100.

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: state of the art and future research directions. International Journal of Production Research, 57(7), 2179-2202.

Behzadi, G., O'Sullivan, M. J., Olsen, T. L., & Zhang, A. (2018). Agribusiness supply chain risk management: A review of quantitative decision models. Omega, 79, 21-42.

Behzadi, G., O'Sullivan, M. J., Olsen, T. L., Scrimgeour, F., & Zhang, A. (2017). Robust and resilient strategies for managing supply disruptions in an agribusiness supply chain. International Journal of Production Economics, 191, 207-220.

Bellantuono, N., Pontrandolfo, P., & Scozzi, B. (2018). Guiding materiality analysis for sustainability reporting: the case of agri-food sector. International Journal of Technology, Policy and Management, 18(4), 336-359.

Bode, C., Wagner, S. M., Petersen, K. J., & Ellram, L. M. (2011). Understanding responses to supply chain disruptions: Insights from information processing and resource dependence perspectives. Academy of Management Journal, 54(4), 833-856.

Bowrey, G., & Clements, M. (2019). Supply Chain Legitimation through CSR Reporting. Australasian Accounting, Business and Finance Journal, 13(1), 27-43.

Carbonara, N., & Pellegrino, R. (2017). How do supply chain risk management flexibility-driven strategies perform in mitigating supply disruption risks? International Journal of Integrated Supply Management, 11(4), 354-379.

Carr, A. S., Kaynak, H., Hartley, J. L., & Ross, A. (2008). Supplier dependence: impact on supplier's participation and performance. International Journal of Operations & Production Management.

Chaudhuri, A., Boer, H., & Taran, Y. (2018). Supply chain integration, risk management and manufacturing flexibility. International Journal of Operations & Production Management.

Chen, I. J., & Kitsis, A. M. (2017). A research framework of sustainable supply chain management. The International Journal of Logistics Management.

Chen, L., Zhao, X., Tang, O., Price, L., Zhang, S., & Zhu, W. (2017). Supply chain collaboration for sustainability: A literature review and future research agenda. International Journal of Production Economics, 194, 73-87.

Chepleting, F., & Musau, E. (2019). Influence of supply chain Risk Reduction on performance of Kenya beverage industry: A case of Almasi Beverages Limited, Eldoret. The Strategic Journal of Business & Change Management, 6(2), 2533-2539.

Chepleting, F., & Musau, E. (2019). Influence of supply chain Risk Reduction on performance of Kenya beverage industry: A case of Almasi Beverages Limited, Eldoret. The Strategic Journal of Business & Change Management, 6(2), 2533-2539.