The International Journal of Business Management and Technology, Volume 5 Issue 3 May–June 2021
ISSN: 2581-3889

Research Article Open Access

Policy Framework for Cyber Security Concernsand Performance of Small and Medium Enterprises for Global Economic Recovery amidst Covid-19

[1]Dr. Evans Mwasiaji*, [2]Dr. John M. Kandiri& [3]Prof. David M. Minja
[1]*Department of Business Administration, Kenyatta University. Nairobi – Kenya.*
[2]*Department of Computing and Information Technology, Kenyatta University, Nairobi – Kenya.*
[3]*Department of Public Policy and Administration, Kenyatta University, Nairobi – Kenya.*

Abstract: Coronavirusdiseaseoutbreak of 2019 was first reported during the month of December in Wuhan City, Hubei Province of China. Due to the changing nature of the disease, governments and regulatory agencies globallyimplemented containment measures includingsocial distancing, quarantines and cessation of movement. Theseglobal response strategies made it necessary for small and mediumbusiness enterprises to turn to digital media to run their operations.E-commerce throughcloud computing became the most viable tools to continue running operations. The adopted e-commerce solutions and cloud based storage integration has attracted integrity and privacy concerns due to the cyber security threats.Cyber criminals have enhanced their assault on vulnerable small and medium firms, taking advantage of their inadequate experience with technology and lack of access to strategic resources such as finance. This studyusing meta-analysis approach thereforepropose a conceptual model that is meant to inform future studies that will seal data gaps, help reconfigureonline data infrastructure, build capacity for entrepreneurs and provide policy solutionsto address cybersecurity so as toenhance contributions by e-commerce compliant small and medium business enterprisesforeconomic recovery within the context of coronavirus disease outbreak.

KeyWords: *Cyber Security,Policy Framework,Cloud-computing,COVID-19, SMEs.*

I. INTRODUCTION

The growth and development of Small and Medium Enterprises (SMEs)issaid to be useful as an engine of job creation and promotion of sustainable economic development (OECD, 2019; British Crown, 2019: UN, 2017). The outcome of this isenhanced standard of living for communities due to commercialization of innovations and poverty assuagement connected to entrepreneurship(Weinberger, Wach, Stephan &Wegge, 2018; Department of Parliamentary Services. 2018; Laura, 2020). The SME sector is also considered a training ground for entrepreneurs,a channel for mobilizing local savings andfor ensuring a more equitable distribution of income (Kongmanila&Kimbara 2011). With increased job losses attributed to harsh economic conditions, the SME sector hasbeen considered a possible counteracting force bymaking a significant contribution towards economic recovery, especially in the context of coronavirus disease outbreak (Laura, 2020;Georgia, 2020). Due to their size, the SMEs require a relatively small capital investment for start-up thereby offering a relatively high labour to capital ratio (Lechat& Torres, 2016). In addition, entrepreneurs who pay attention to the triple bottom line in terms of the people, planet and profits ends up improving the society and the environment (Gatukui&Gatuse, 2014). However, the aftermath of coronavirus(COVID-19) disease outbreak showed the financial fragility of firms in the SME sector amplified by disruptions in global supply chains, resulting in mass layoffs and business closures (Mwasiaji, Jagongo & Ogutu, 2020).Previous studies have reported that accomplishment of trade in such an erratic and unreliable business environment is determined by an organization's capability to adjust and respond to environmental variations (Krieger, Block & Stuetzer, 2018; Gatukui & Gatuse, 2014). For SMEs, they have been forced to adopt digital sales channels resultingin cyber securityrelated challenges (Tam, Rao & Hall, 2020; Longbottom, 2020).

Streams of studies in entrepreneurship have for some time now directed their effort in generating empirical data sets to support business performance for national and global economic wellbeing (Krieger, Block &Stuetzer, 2018; Alvarez & Sinde-Cantorna, 2014; Bigliardi, Colacino&Dormio, 2011). The proposed business support programmes have mainly been geared towards formulating a policy framework to reduce business barriers, reward innovation, protection of private property, cushion SMEs in times of crisis and support to stakeholder networking within the SME ecosystem towards the achievement of the 2030 global agenda (Reymen, Andries, Berends, Mauer, Stephan & Van Burg, 2015; De Clercq&Voronov,2011). Unfortunately, not much has been done to examine the impact that cyber security challenges continues to have on SME sector firms within the context of COVID-19 pandemic. There is needtherefore to come up with data driven programmes to address cyber security concernsfor firms, especially those in the SME sector due to

their unique challenges related to their small size (Lechat& Torres, 2016; Tam, Rao & Hall, 2020; Longbottom, 2020).The purpose of this study therefore is to provide a review of extant literature on the perspectives associated with SMEs' cyber security concerns, similar to Facebook and Cambridge analytica data breach, within the context of disruptions caused by COVID-19 disease outbreak.

II. PROBLEM STATEMENT

The World Health Organization (WHO) alerted governments and regulatory authorities globally about COVID-19 outbreak which was identified to be rapidly spreading along international transit routes (WHO, 2020; Bajema, et al., 2020; Mwasiaji, Jagongo&Ogutu, 2020). The consequent global containment strategies including embargos on international flights, total lockdowns, movement restrictions and interruptions in global supply chains resulted in economic and social disruption of many countries around the world(WHO, 2020; GEM, 2020). COVID-19 disease outbreak presented opportunities as well as difficulties for entrepreneurs and policy makers across the world. Opportunities for entrepreneurs include identifying and exploiting new products, process or markets through e-commerce (Berman, 2020; Reymen, Andries, Berends, Mauer, Stephan & Van Burg, 2015). Challenges include business related constraints that forced small and medium enterprises to adopt digital marketing and sales channels to enable them function remotely (Laura, 2020; Jessica, 2020).With business and customer data increasingly accumulating, the adopted e-commerce solutions and cloud based storage integration has become a prime concern due to security threats andprivacy challenges for customers(Tam, Rao & Hall, 2020).Even though amassing of big data by SMEs can enhance customer care services and targeted marketing, unfortunately agile cyber criminals have enhanced their assaults on small and medium enterprises, taking advantage of the chaotic situation and SME's inadequate experience with technology and lack of access to strategic resources such as finance and skills to operationalize ISO 27001 information security management system (Laura, 2020; Ackerman Jr. 2019; Shojaie, 2018; Abualloush, *et al*., 2016).Despite attempts to enhance cyber security, there is still debate about integrity, availability and confidentiality of online data generated during e-commerce transactions (Abualloush, *et al*., 2016; Kuang, 2011).

Some studies have reported that online data storage medium, such as transaction logs and other sensitive information still have security concerns because the auto-tiering method does not keep track of data storage location (Tam, Rao & Hall, 2020; Ackerman Jr., 2019.; Galinec, Možnik & Guberina, 2017). In addition, there is the data breach by hackers who use ransomware to often try to glean information such as credit card numbers or bank account information for sale to the highest bidder (Gagliardi, Hankin, Gal-Ezer, Mc Gettrick & Meitern, 2016).A simple steady security check for datasets for big data cannot detect security patches for continuous streaming data (Broadhurst, Grabosky, Alazab& Chon, 2014). Breach of data through cybercrime may not only expose SMEs to legal suits from customers, but may also affect a firm's competitive position in the form of loss of customer confidence, violation of privacy, ransomware, eavesdropping, stolen business strategies and intellectual property (Roy, 2013; Zeng, *et. al*., (2013). There is need therefore for researchers to develop additional conceptual models upon which cyber security propositions at the abstraction level can be advanced and empirically tested. In the context of SMEs, the effect cyber security on e-commerce is still not fully understood (Tam, Rao & Hall, 2020; Galinec, Možnik&Guberina, 2017).As national and global economies seek to recover from the ravages of COVID-19 pandemic, businesses especially SMEsrequiredata based support programmes and policy framework to facilitate capacity building,reconfiguration of online data infrastructure so as to insulate themselves from cyber criminals (Cutler & Summers, 2020;Tam, Rao & Hall, 2020; Longbottom, 2020;Alqahtani, 2017; Bruijn& Janssen, 2017). This paper is meant to provide a prescriptive model to address cyber security challenges to enable the SMEs to moreeffectively play their role given their contribution towards economic wellbeing at the local and international level.

III. REVIEW OF PERTINENT LITERATURE

3.1 Impact of COVID-19 Pandemic on SME sector Firms

COVID-19 disease outbreak was first reported during the month of December 2019 in Wuhan City, Hubei Province of China (WHO, 2020).A subsequent public health emergency was declared by the Centre for Disease Control and Prevention in the United States on 31stJanuary 2020 (Bajema, et al., 2020).The first and second wave of the COVID-19 witnessed geographical contagion from Asia to other parts of the world and the market panic due to supply chain disruptions and the projected high economic cost of the pandemic (Darab, *etal,* 2021; Bartik, *et al*., 2020). Forecasts issued showed a negative economic outlook with a 6% reduction in global GDP, and a 7.6% drop as a result of a second pandemic wave by end 2020, with some of the most affected countries registering a double digit fall(OECD, 2020).Due to the rapidly evolving nature of COVID-19 pandemic, governments and regulatory agencies around the world had to continue implementing containment measures with serious economic implications. For instance, the global pandemic containment strategies had an immediate impact on the international supply chains in terms of the different processes and activities that make it possible for goods and services to get to the end users (GEM, 2020; Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020). For instance, COVID-19 containment measures resulted in lead times in some cases doubling and supply shortages occasioned by movement restrictions along the supply chains (Berman, 2020). These disruptions impacted different individuals, societies and organizations in varying proportions (Darab, *etal,* 2021; Bartik, *et al*., 2020; Longbottom, 2020). The demand side of business enterprises for instance experienced severe drops in capacity utilization due to lockdowns and quarantines measures put in placeto contain the pandemic.

Thesudden loss of demand and revenue for SMEs severely affect their ability to function due to major liquidity shortages (OECD, 2020).In addition, supply chains were in most cases interrupted leading to shortages of parts and intermediate goods (Mwasiaji, Jagongo&Ogutu, 2020).Many potential consumers also experienced loss of income, fear of COVID-19 contagion and heightened uncertainty, which resulted in reduced spending and product consumption (Berman, 2020). The situation was made worse by job losses by salaried employees, resulting in reduced business and consumer confidence (IMF, 2021; GEM, 2020; Mwasiaji, Jagongo&Ogutu, 2020).Previous studies have reported that SME sector firms are more likely to be impacted by economic turbulence in greater proportion as compared to their larger counterparts because of their inherent weaknesses (OECD, 2020; Kucharski, *et. al*, 2020).SME sector firms have to cope with the constrictions that are three fold in nature. Some are connected to their small sizes and resource capabilities. Being small in size imposes costs and innovative penalties in the areas of technology, marketing and sales channels, due to lack of economies of scale (Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020). Some constrictions arise from market distortions, while others are an offshoot of policy interventions. Financial institutions and providers of productive factors such asinfrastructure, prefer to deal with a few larger entities for safety and economic viability reasons as compared to numerous SMEs with very diversified needs and characteristics (Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020; Department of Parliamentary Services, 2018; Krieger, Block &Stuetzer, 2018). The argument is that SME sector firms are more difficult to collect comprehensive information on them, for decision making, such as to facilitate credit rating. SMEs are also said to be more difficult to monitor and the cost of enforcing contracts may be disproportionately large as compared to the size of the transaction (Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020; Cutler & Summers, 2020; Hitch, 2020; Longbottom, 2020).

With COVID-19 restrictions in place for containing the pandemic, SMEs therefore have lessflexibility and resilience in managing the direct and indirect financial implications brought about by a sudden shift in factors within the operating environment such as those brought about by COVID-19 disease outbreak (GEM, 2020). Costs incurred as a result of underutilized capacity and changes in work processes to adopt e-commerce and remote working weighs higher for SME sector forms considering their low level of digitization and difficulties in accessing strategic resources. SMEs may also find it challenging to access information on viable strategies for managing the economic shocks, including available government support programmes to lighten the economic burden (Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020; Cutler & Summers, 2020; Hitch, 2020).This means that the viability of SME sector firms is at a greater financial risk under COVID-19 pandemic.Although recent vaccine approvals have raised hopes of economic turnaround, renewed waves and new variants of severe acute respiratory syndrome coronavirus COVID-19 virus 2 pose concerns for the outlook (IMF, 2021; OECD, 2020; Cutler & Summers, 2020). Returning SMEs back to operational health post COVID-19 restrictions will therefore be very challenging since they traditionally rely on limited cash reserve as compared to their larger counterparts (IMF, 2021; JP Morgan, 2016). Many will need to reactivate their entire supply chains while digitizing processes to mitigate against future disruptions in multiple geographies. Unfortunately the third wave is just hitting and due to possible lack of available credit and broken supply chains, there is likely to be an increased pressure primarily on SME sector firms.

3.2E-commerce Security Concerns and Entrepreneurial Capabilities

The international COVID-19 containment measures put in place made it necessary for SMEs to adopt digital marketing and sales channels in order to function remotely (Longbottom, 2020; Bartik, Bertrand, Cullen, Glaeser, Luca& Stanton, 2020). With business and customer data increasingly accumulating in terms of volume, variety, velocity and value, the adopted e-commerce solutions and cloud based storage integration continues to be a prime concern due to cyber security threats andprivacy challenges for customers (Tam, Rao & Hall, 2020).Cyber criminals have enhanced their assault on firms with serious implications especially for SMEs, taking advantage of their lack of access to strategic resources such as finance and expertise in cyber skills (Ackerman Jr. 2019; Longbottom, 2020). Cyber security attacks in the early phases of the pandemic included more than 907 thousand Spam messages, 737 Malware attacks and 48 thousand hits on malicious links around the world as of April 2020 (Trendmicro, 2020). In the month of March 2020, there were 220 times increase in spam email and 260% in malicious URLs with most of the target online users accessing them from the United States (Trendmicro, 2020). Many governmental regulatory agencies and healthcare related firms for instance have witnessed an increase in the Distributed Denial of Services attack (Khan, Brohi&Jhanjhi, 2019). Cybercriminals have also been taking advantage of the COVID-19 situation by spreading Malware, Spywares and Trojans through embedded interactive coronavirus maps and websites (MalwareBytes, 2021). A major operation method by cyber criminals is to attempt to lure users into clicking on an email link or downloading the malware from spam emails, for which the user becomes a victim through mobile device or computers (Interpol (2020). There has also been an increase in online platforms that claim to be applications to protect users from coronavirus disease (MalwareBytes, 2021; Peterson, 2020). There have also been concerns about user privacy policies by online organizations, including claims that applications such as Google Meet, Microsoft Team and Zoom that have become handy during the pandemic may be collecting more data than people realize (St. John, 2020).

The effects of cybercrimes continue to have serious negative implications for individual customers and business enterprises in terms of identity theft, cyber bullying and stalking, denial of service attack that takes over a firm's online platform, computer viruses, transaction fraud, security costs and immense monetary losses (Hayashi, 2013; St. John, 2020; Trendmicro, 2020; Longbottom, 2020). Old methods required for doing business within the context of COVID-19 pandemic may no longer be available, and new mechanisms and capabilities for trade through e-commerce

may be required (Mwasiaji, 2020). Since more and more organizations have adopted e-commerce in order to gain competitiveness in terms of enhanced customer interaction efficiency through online registration, content personalization and real-time online support, there is need for deployment of e-commerce entrepreneurial capabilities leads to enhanced organizational financial performance (ITC, 2016; Shah, *et. al.,* 2007). Similarly, Merono-Cerda and Soto-Acosta (2007) established a correlation between e-commerce capability allocation and strong financial performance of a business enterprise. Entrepreneurial e-commerce competencies are therefore the knowledge and skills needed to develop, sustain and lead a business organization (Mwasiaji, 2020; Marvel *et al.,* 2016). The more developed an entrepreneur's skills, the better able to respond to environmental forces so as to grow and sustain the business in the digital era. An entrepreneur should have knowledge of the market, of relevant technologies or of how to run a firm. Therefore, it can be taken that relevant knowledge and skills set is an important predictor of entrepreneurial outcomes (Krieger, *et. al.,* 2018).

3.3Policy Framework for E-Commerce

Cybercrimes are globally estimated to cost an annual economic investment of about six (6) trillion US$ (Lubua& Pretorius, 2019). This estimate suggests an increase in cyber security related threats to enterprises and individual end users of products purchased online (Saunders, 2017; Herjavec Group, 2017; Alqahtani, 2017). About half of all online attacks are directed at SME sector firms (Dawson, 2018; Herjavec Group, 2017;Bendovschi, 2015). The situation is likely to be more alarming within the context of COVID-19 pandemic given that more SMEs have had to adopt digital marketing and sales channels to overcome the traditional face – face business challenges due to the global pandemic containment measures (Tam, Rao & Hall, 2020; Cutler & Summers, 2020; Longbottom, 2020). The SME sector cyber related threats have been exuberated by both internal and externally oriented challenges. Internal difficulties include low level of management and digital skills, while external difficulties include inadequate cyber security regulations, coupled with complicated legal framework and inefficient judicial bureaucracy (Tam, Rao & Hall, 2020; Herjavec Group, 2017; Alqahtani, 2017). Without resolving the SME cyber related challenge areas, the contributions of the sector to economic recovery post – COVID pandemic may not be maximised (Tam, Rao & Hall, 2020; GEM. 2020).

In view of challenges of e-commerce adoption at the global level, the United Nations in 1996 adopted the UNCITRAL (United Nations' Commission on International Trade Law) Model Law on Electronic Commerce (UN, 1998; Dawson, 2018). This was to serve as pioneer e-commerce legislation for countries across the world to duplicate and domesticate in their respective jurisdictional areas, including establishing relevant institutions that conform substantially to the provisions of the Model Law. A key objective of UNCITRAL was to eliminate obstructions as well as barriers on the way of electronic documentation, especially regarding their enforceability before law courts (UN, 1998; Shojaie, 2018; Alqahtani, 2017; Atoum, Otoom& Ali, 2014). For instance, e-signature and e-contract laws were to be put in place to facilitate cross-border e-signature recognition and international e-payments to facilitate online business, with reasonable security practices and procedures and sensitive personal data (UN, 1998; ITC, 2015; Alqahtani, 2017; OECD, 2019).International e-payments also required an enabling regulatory framework on cross-border transfer of foreign exchange and more so the prevention and detection of cybercrimes committed through online platforms (UN, 1998; OECD, 2020). Lastly, e-commerce demand rules for consumer protection (ITC, 2015; Sokobe, 2015; Alqahtani, 2017). The Model Law therefore geared towards creating uniformity of e-commerce standards and practices among member states to facilitate cross boarder e-commerce (UN, 1998; Alqahtani, 2017). While e-commerce can enhance the inclusion of SMEs in global markets, it also risks producing the opposite outcome especially within the context of COVID-19 pandemic because of the digital gap between the SMEs and large firms (Tam, Rao & Hall, 2020).

While governments take a more active role in shaping economic activity post COVID-19, there is need to formulate and implement policies and regulations supportive of SMEs to avoid, mitigate and pre-empt a future social and economic crisis of similar magnitude. This is because of the critical role of the SME sector in the growth and development of national economies. Specific policy recommendations for increasing SMEs' adoption of digital marketing and sales solution follow directly from the discussion above. This paper is of the view that there is need for Cybersecurity policy framework to be developed to provide specific guidelines for education and training policies for improving the relevant entrepreneurial competencies to improve SME access to e-payment systems, but also cyber security. There is also need for public policy for risk based cyber security management practices for SME sector firms including carrying out risk analysis on data to identify threat source, threat events, vulnerabilities, likelihood of occurrence and impact. Policy should encourage and facilitate SMEs to have in place online security protocols requiring authorization of online transactions to be preceded by authentication so as to ensure that e-commerce and customer data is protected from disclosure or modification.

3.4 Adoption of Technology Theories

Several theories have been advanced seeking to explain the adoption of technological innovations by the society. Rogers (1962) Diffusion of innovation theory is one of the oldest social science theories that attempts to explain how an idea or product gains momentum over time as it spreads through specific populations and communities. According to Rogers (1962), adoption happens when a person perceives an idea as innovative before diffusion takes place. The diffusion of the innovation does not happen uniformly across the society, but rather some people adopt an innovation earlier than others. In a similar line of enquiry, the Unified theory of acceptance is another theory of acceptance of technological innovations (Venkatesh, Thong & Xu, 2016). According to Oshlansky, *et. al.,* (2007), this theory that seeks to explain user intention to adopt technology, has a higher explanatory power on innovation

acceptance as compared to other technology propositions. Venkatesh, *et al.,* (2003) study identified conducive factors as one of the constructs that impacts on an individual's perception and user behaviour.

Wernerfelt(1984) Resource Based View (RBV) model has also been applied in seeking to explain a variety of phenomena including information systems. The RBV model identifies an organization's internal resources as a driver for obtaining competitive advantage (Santhanam& Hartono, 2003; Wade &Hulland, 2004). Peteraf (1993) used RBV model to examine the relationship between Information Technology and e-commerce capabilities and their influence on firm performance. The study concluded that e-commerce business value is more derived from a firm's internal skills and capability to align technological innovations to a firm's strategic objectives, rather than the adopted technology in itself (Lee *et. al.,* 2012). This conclusion was also supported by Powell (2001) who proposed that the focus of inquiry changed from the structure of the industry to the firm's internal structure, resources and capabilities. These theories raise pertinent issues that have implications on SMEs' adoption of e-commerce. They can also be used to better understand the manner and speed of digitization including the small business entrepreneurs' decisions to adopt e-commerce and related technology to achieve a competitive advantage.

IV. STUDY METHODOLOGY

This study adopted a meta-analysis approach in collecting and critical review of secondary data from research findings of other studies based on primary data (Glaszious, 2001).The strategy used to search data and data bases included visiting electronic databases and identifying relevant articles, snowballing of the literature and articles by moving from one journal to another searching for relevant literature, and by asking subject experts to help identify relevant sources. This studytherefore interrogated and interpreted available literature evidence from other empirical studies to gain an understanding of cyber security concerns particularly for SME sector firms (Paterson, Thorne, Canam&Jillings, 2001).

V. PROPOSED CONCEPTUAL MODEL

The following is the proposed conceptual model that demonstrates the role of entrepreneurial competencies and policy framework on the link between cyber security and performance of SMEs within the context of COVID-19 disease outbreak.

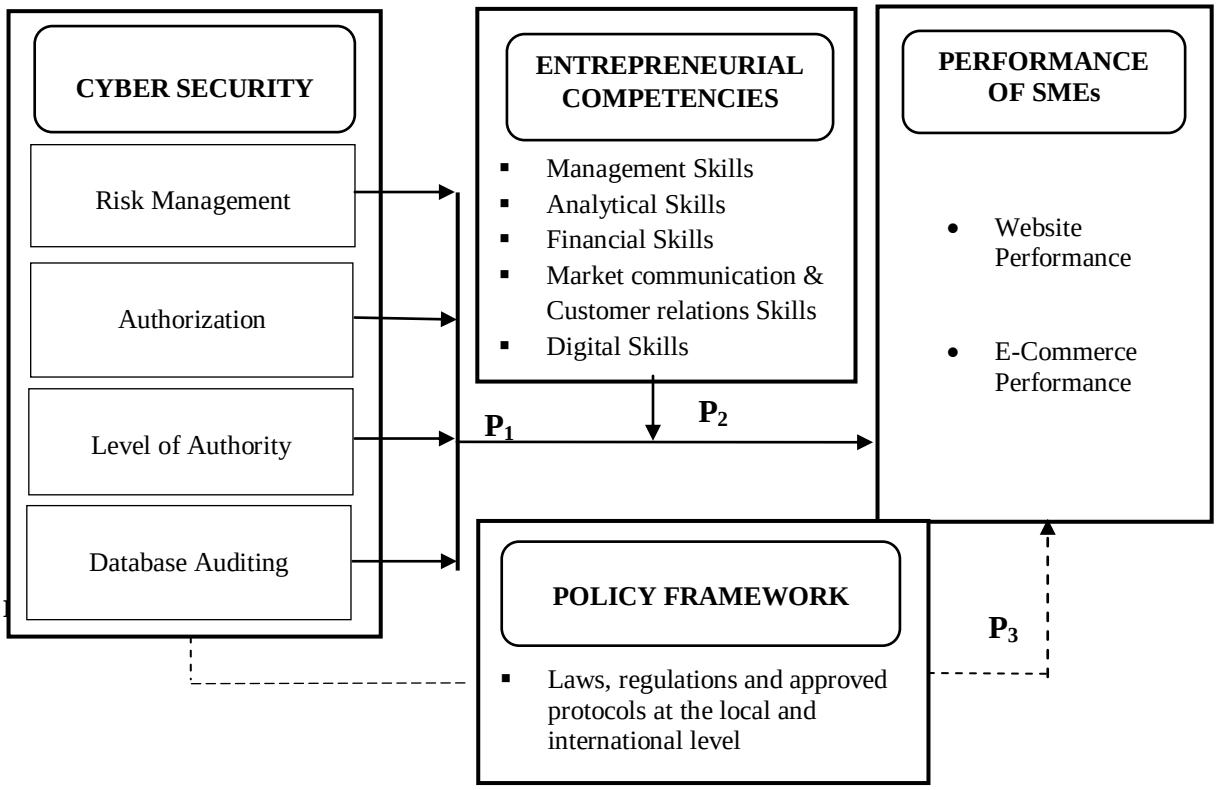

Figure 1: *A conceptual Model for Cyber Security, Entrepreneurial competencies, Policy Framework and SME performance.*

5.1 Propositions

5.1.1 Cyber Security

Global response strategies for COVID-19 disease outbreak made it necessary for SMEs to adopt digital sales channels to function remotely (Laura, 2020; Jessica, 2020). E-commerce has therefore become the new frontier for SMEs in a globalised business environment (GEM, 2020). With business and customer data increasingly accumulating, the adopted e-commerce solutions and cloud based storage integration for competitive advantage has become a prime concern due to cyber security threats andprivacy challenges for customers (International Trade Centre, 2015).). Consistent with empirical studies reviewed in this paper, the study proposes that:

Proposition 1(*P1*): *There is a relationship between Cyber Security and Performance of SMEs.*

5.1.2 The role of Entrepreneurial Competencies

There is need for entrepreneurship competencies to identify an opportunity, develop, innovative and successfully lead a business. SME sector entrepreneurs should possess relevant competencies such as knowledge of the market, how to run a firm and relevant ICT infrastructure and digital skills (Henry, Hill & Leitch, 2004; Sinha, *et. al.,* 2011; Mwasiaji, 2020). Therefore, it can be summarized that relevant knowledge and skills set is an important predictor of performance of SME sector firms (Krieger, *et. al.,* 2018). Based on this, the study proposes that:

Proposition 2 (P2): *Entrepreneurial competencies mediate the relationship between Cyber Security and Performance of SMEs.*

5.1.3 The Role of Policy Framework

Policy framework is the regulatory environment in which SME sector businesses operates and which can directly or indirectly impact on their operations (Gonzalez-Torre &Adenso-Diaz, 2010). From the Conceptual model, the dotted line P3 influencesthe relationship between cyber security and performance of SMEs. Consistent with both conceptual and empirical literature reviewed in this study, it is proposed that:

Proposition 3 (P3): *Policy Framework moderates the relationship between Cyber Security and Performance of SMEs.*

VI. CONCLUSIONS

This study reviewed extant literature, identify gaps in the phenomenon of Cyber security, entrepreneurial competencies, policy frameworkand performance of SMEs within the context of COVID-19,and finally proposed a conceptual model providing propositions for filling up the identified gaps. The reviewed works show that adoption of digital sales channels to function remotely has an influence on performance of SMEs as they seek to play their role in post - coronavirus disease outbreak of 2019 economic recovery. After reviewing results of relevant studies, it is concluded that there is a relationship between cyber security and website performance and e-commerce performance of SMEs whether directly or indirectly. This study cannot neglect the relation and its impact on SMEs in view of their critical role in economic wellbeing at local and international levels. It is proposed that more studies should be undertakento clarify their nature of relations. This study therefore proposes a conceptual model as a basis for studies to seal data gaps and help reconfigure online data infrastructure and policy solutions to address cyber security threats. Empirical data will also be useful in the formulation of capacity building guidelines and standard operating procedures that focuses on identifying, analysis and management of risk by e-commerce compliant SMEs for economic recovery within the context of coronavirus disease outbreak.

ACKNOWLEDGEMENT

We would like to acknowledge the support by all the subject experts who provided advisefor this study, including the Kenyatta University Management in availing a postmodern library for review of literature relevant to this study. To all those who contributed in one way or another in actualizing this study, and whom we may not individually mention by name, we highly appreciate your contributions.

REFERENCES

[1.] Alvarez, G., &Sinde-Cantorna, A. I. (2014). Self-employment and job satisfaction: An empirical analysis. International Journal of Manpower, 35(5), 688–702.

[2.] Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. Procedia Computer Science, 124(1), 691–697.

[3.] Atoum, I., Otoom, A., & Ali, A. A. (2014).A holistic cyber security implementation framework. Information Management & Computer Security, 22(3), 251-264.

[4.] Ackerman Jr. R., (2019). The Cyber Skills Shortage Continues to Balloon—And Think Tanks Aren't Helping. Retrieved from https://www.rsaconference.com/industry-topics/blog/the-cyber-skills-shortage-continues-to-balloon-and-think-tanks-arent-helping

[5.] Bajema, K.L., et al., (2020). Persons evaluated for 2019 novel coronavirus— United States, January 2020, Morb. Mortal. Wkly. Rep., vol. 69, no. 6, p. 166, 2020.

[6.] Bartik, A.W., Bertrand, M., Cullen, Z., Glaeser, E.L., Luca, M. & Stanton, C. (2020).The impact of COVID-19 on small business outcomes and expectations.Proceedings of the National Academy of Sciences of the United States of America. PNAS 117 (30) 17656-17666.

[7.] Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28(1), 24-31.

[8.] Bigliardi, B., Colacino, P., &Dormio, A. I. (2011). Management & Innovation: Innovative Characteristics of Small and Medium Enterprises, Butterworth-Heinemann, Amsterdam.

[9.] British Crown (2019). Business Population Estimates for the UK and Regions. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/254552/13-92-business-population-estimates-2013-stats-release-4.pdf.

[10.] Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. International Journal of Cyber Criminology, 8(1), 1-20.

[11.] Bruijn, H., & Janssen, M. (2017).Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), 1-7.

[12.] Cutler, D.M. & Summers, L.H. (2020).The COVID-19 Pandemic and the $16 Trillion Virus.*JAMA*. 324 (15): 1495-1496. doi:10.1001/jama.2020.19759

[13.] Darab, M.G., Keshavarz, K., Sadeghi, E., Shahmohamadi, J. & Kavos, Z. (2021).The economic burden of coronavirus disease 2019 (COVID-19): evidence from Iran BMC Health Services Research volume 21, Article number: 132

[14.] Dawson, M. (2018).Applying a holistic cybersecurity framework for global IT organizations. Business Information Review, 35(2), 60-67.

[15.] Department of Parliamentary Services.(2018). Small Business Sector Contribution to the Australian Economy. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/6272043/upload_binary/6272043.pdf

[16.] Gagliardi, F., Hankin, C., Gal-Ezer, J., McGettrick, A., &Meitern, M. (2016).Advancing Cybersecurity Research and Education in Europe. New York: Association for Computing Machinery.

[17.] Galinec, D., Možnik, D., &Guberina, B. (2017). Cybersecurity and cyber defence: national level strategic approach. Automatica, 58(3).

[18.] Gatukui, P. K., &Gatuse, P. (2014). A review of SMEs strategic planning for growth and sustainability in Kenya: Issues and challenges. International Journal of Social Sciences and Entrepreneurship 10, no. 1: 26-41.

[19.] GEM (2020).Diagnosing COVID-19 Impacts on Entrepreneurship.Global Entrepreneurship Research Association, London Business School, Regents Park, London NW1 4SA, UK ISBN (print): 978-1-9160178-4-9 ISBN (ebook): 978-1-9160178-5-6

[20.] Glasziou, P. (2001) Systematic Reviews in Health Care: A Practical Guide.New York, NY: Cambridge University Press.

[21.] Hitch, G.,(2020). Big four banks to speed up loans for businesses applying for Job Keeper amid coronavirus crisis, Josh Frydenberg says. *ABC News* (Apr. 2020). Retrieved on June 18, 2020 from https://www.abc.net.au/news/2020-04-23/banks-agree-speed-up-loans-for-businesses-waiting-for-jobkeeper/12176632

[22.] International Monetary fund (2021). Economic Outlook Report.Retrieved on April 2, 2021 from https://www.imf.org/en/Publications/WEO/Issues/2021/01/26/2021-world-economic-outlook-update

[23.] Interpol (2020).“COVID-19 cyberthreats,” [Online]. Available: https://www.interpol.int/en/Crimes/Cybercrime/COVID-19- cyberthreats. [Accessed: 04-April-2021].

[24.] International Trade Centre (ITC) Bringing SMEs onto the e-Commerce Highway Geneva: ITC, 2016.xiii, 101 pages Doc. No. OCE-16-13.E

[25.] JP Morgan (2016). Cash Is King: Flows, Balances, and Buffer Days—Evidence from 600,000 Small Businesses. Retrieved on 3rd April 2021 from https://institute.jpmorganchase.com/content/dam/jpmc/jpmorgan-chase-and-co/institute/pdf/jpmc-institute-small-business-report.pdf

[26.] Khan, N. A., Brohi, S. N. &Jhanjhi.NZ, (2019). “UAV’s Applications Architecture Security issues and Attack Scenarios: A Survey,” in 1st International Conference on Technology Innovation and Data Sciences (ICTIDS).

[27.] Krieger, A., Block, J. &Stuetzer, M. (2018). Skill variety in entrepreneurship: A literature review and research directions. International Review of Entrepreneurship, 16(1), 29-62.

[28.] Laura, H., (2020). Small Businesses Drive China's Economy: The Coronavirus Outbreak Could Be Fatal for Many. (February 2020) Retrieved on March 29, 2021 from https://edition.cnn.com/2020/02/14/economy/coronavirus-china-economy-small-businesses/index.html.

[29.] Longbottom, J., (2020). Coronavirus Forces Businesses to Adapt to Survive the COVID-19 Pandemic. (March 2020) Retrieved on March 22, 2020 from https://www.abc.net.au/news/2020-03-19/how-businesses-adapting-to-survive-covid-19-coronavirus/12068696.

[30.] Lubua, E.W. & Pretorius, P.D. (2019).Cyber-security Policy Framework and Procedural Compliance in Public Organisations. Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, Czech Republic, July 23-26, 2019

[31.] OECD (2019).OECD Digital Economy Outlook 2020. OECD Publishing, Paris. Retrieved on 2nd April 2021 from http://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm

[32.] MalwareBytes (2021). “Fake ‘Corona Antivirus’ distributes BlackNET remote administration tool.” Available: https://blog.malwarebytes.com/threat-analysis/2020/03/fake-coronaantivirus-distributes-blacknet-remote-administration-tool/. [Accessed: 04-April-2021].

[33.] **Mwasiaji, E. (2020).** Product Development and Process Improvement in Small and Medium Food Manufacturing Firms in Nairobi City County, Kenya. SSRG *International Journal of Economics and Management Studies, 7(1), 18-29. ISSN: 2393-9125. DOI: 10.14445/23939125/IJEMS-V711P103*

[34.] Mwasiaji, E., Jagongo A.O. &Ogutu J.O. (2020). Coronavirus Disease Outbreak and the Supply Chain of Selected Small and Medium Manufacturing Enterprises in Kenya: International Journal of Business and Social Science, 11(4), 7-16. ISSN: 2219-6021. DOI: 10.30845/ijbss.v11n4a2

[35.] Paterson, B.L., Thorne, S.E., Canam, C. &Jillings, C. (2001). Meta-study of qualitative health research: A practical guide to meta-analysis and meta-synthesis. London: Sage publications.

[36.] Peterson, P., (2020). "Business Email Compromise (BEC): Coronavirus a Costly New Strain of Email Attack," Available: https://www.agari.com/email-security-blog/business-emailcompromise-bec-coronavirus-covid-19/. [Accessed: 04-April-2021].

[37.] Redrup, Y., (2020). Beverage maker Lion hit by cyber-attack. *Finance. Rev.* (Jun. 2020). Retrieved on March 29, 2021 from https://www.afr.com/politics/federal/super-early-access-frozen-amid-afp-fraud-investigation-20200508-p54r1z.

[38.] Shojaie, B. (2018). Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different Culture. Hamburg: Universitat Hamburg. Retrieved April 4, 2021, from http://ediss.sub.uni-hamburg.de/volltexte/2018/9005/pdf/Dissertation.pdf

[39.] St. John, A., (2020). "It's Not Just Zoom. Google Meet, Microsoft Teams and Webex Have Privacy Issues Too., "Available at: https://www.consumerreports.org/video-conferencingservices/videoconferencing-privacy-issues-google-microsoftwebex/. [Accessed: 04-April-2021].

[40.] Sokobe O.E. (2015). 'Factors influencing adoption of electronic payment by small and medium hotel enterprises in Kisii town, Kisii County, Kenya'.

[41.] Tam, T., Rao, A. & Hall, J. (2020).The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath.Digit. Gov.: Res. Pract., Vol. 2, No. 2, Article 23, Publication date: December 2020.DOI: https://doi.org/10.1145/3436807

[42.] Trendmicro (2020). "Developing Story: COVID-19 Used in Malicious Campaigns," Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrimeand-digital-threats/coronavirus-used-in-spam-malware-file-names- and-malicious-domains. [Accessed: 04-April-2021].

[43.] United Nations (1998). UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998. Retrieved on 3rd April 2021 from https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-04970_ebook.pdf

[44.] Venkatesh, V., Thong, J.Y. L. & Xu, X. (2016) "Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead," Journal of the Association for Information Systems: Vol. 17: Issue 5, Article 1. DOI: 10.17705/1jais.00428 Available at: https://aisel.aisnet.org/jais/vol17/iss5/1

[45.] World Health Organization (2020).Coronavirus disease (COVID-19) pandemic. Geneva, Switzerland. https://www.who.int/emergencies/diseases/novel-coronavirus-2019