SSRG International Journal of Computer Science and Engineering
ISSN: 2348 – 8387 / https://doi.org/10.14445/23488387/IJCSE-V8I8P101

Volume 8 Issue 8, 1-7, August 2021

Original Article

Cyber Security Concerns and Competitiveness for Selected Medium Scale Manufacturing Enterprises in the Context of Covid-19 Pandemic in Kenya

Evans Mwasiaji[1], Kenneth Iloka[2]

[1]*Department of Business Administration, School of Business, Kenyatta University*
[2]*Department of Computing and Information Technology (CIT), Kenyatta University*

Received: 02 July 2021 Revised: 06 August 2021 Accepted: 18 August 2021 Published: 25 August 2021

Abstract *- This study hence sought to establish data security concerns for selected medium-scale manufacturing enterprises in Kenya. A descriptive research design was adopted in obtaining data from 76 senior executives. The study recorded a 63.33% response rate, with 67% of the enterprises reporting having experienced a cyber-related incident within the last one year. Intellectual property theft was the most cited cyber security threat at 38%, followed by phishing (24%) and malware (22%). Despite this, only about 6% of the executives are conversant with the applicable data security laws in the country, while 50% are not sure whether their enterprises' cyber risk management program and capabilities are aligned with industry standards. The study concluded that cybercrime is a global problem that exposes businesses to legal suits by customers due to data breaches and may inhibit a firm's competitiveness due to loss of customer confidence, stolen business strategies and intellectual property. There is a need, therefore, for governments globally to collaborate in facilitating capacity building for entrepreneurs and partner in providing policy solutions to address cyber security. This would enhance contributions by e-commerce-compliant businesses towards global sustainable development.*

Keywords *- Cyber security, Medium scale manufacturing enterprises.*

1. Introduction

A resilient small and medium enterprise (SME) sector is a key route for long-term economic development and increased citizen welfare around the world ([1], [2], [3], [4]). This is because small and medium-sized businesses play a key role in job creation, wealth growth, and poverty reduction ([5], [6]). The SME sector also can earn foreign currency and improve regional economic balance through industrial dispersion ([2], [7]). Furthermore, the SME sector is a vital and dynamic component of the private sector, whose entrepreneurial viability is key in fostering national economy responsiveness ([8], [3]). Despite the significance of the SME sector as a whole for economic development, most studies on firm performance focus on micro, small, and large size companies in connection to macroeconomics and government-industrial policies ([2], [4]). This means that there is a gap in the literature on medium-sized businesses, as there is not enough to account for the distinctive nature of their activities and issues ([9], [2]). Construction, quarrying, and mining industries make up the remaining two-thirds of Kenya's industrial sector ([10], [11]). Medium-sized businesses are prevalent in sub-sectors of the manufacturing industry, such as textiles, food, non-metallic products, drinks, apparel and footwear, wood and wood products; pulp, paper, and publishing; plastic and rubber; iron and steel; and pulp, paper, and publishing [12]. The Kenyan government understands that industrialization is a major goal for achieving Vision 2030 and that the manufacturing industry is a critical pillar in achieving this aspiration because of the contribution of the industrial sector to the Gross Domestic Product [10].

While the actual contribution of individual medium-sized manufacturing firms to long-term economic development varies due to their diversity, the manufacturing sector as a whole has not grown as expected due to a variety of factors, including low capital investment, the use of obsolete technologies, high operating costs, and increased competition from cheaper imports ([10], [2], [3], [1]). According to Parliament Budget Office [13], the manufacturing sector's main goal is to assist job creation through improved value addition and to enhance manufacturing's contribution to GDP to 15% by 2022. Despite this goal, the manufacturing value addition sector's share of GDP has continuously dropped from 12 percent in 2009 to around 9 percent in 2019, implying that many of the manufacturing pillar's important projects may not meet their targets for 2020/2021 and the medium term [13]. The international response strategies to the coronavirus disease (COVID-19) outbreak had an impact on the network of

organizations that are involved in the various processes and activities that produce value in the form of products and services in the hands of the ultimate end users through upstream and downstream linkages [14]. COVID-19 reaction measures necessitated the adoption of e-commerce solutions by SMEs. This opened up a slew of new opportunities while also exposing the world to unprecedented cyber risks ([15], [16]). The adoption of e-commerce has undoubtedly resulted in the phenomenon of big data, which is nothing new for multinational corporations but poses a difficulty for SMEs due to the potential of hackers infiltrating networks to launch cyber-attacks [17]. Despite the efforts of various studies to illustrate the significance of digital media adoption, there is still a controversy about the confidentiality and integrity of massive data generated by e-commerce platforms ([16], [17], [18], [19], [20], [21], [22], [23]). As a result, the current study looked into cyber security concerns for Kenyan medium-sized manufacturing businesses in the aftermath of the COVID-19 illness epidemic.

2. Problem Statement

The coronavirus disease outbreak of the year 2019 was first reported in Wuhan City, Hubei province of the People's Republic of China, in the month of December [24]. Governments around the world subsequently started implementing containment measures such as embargos on international flights, total lockdowns and movement restrictions resulting in the economic and social transformation of many countries around the world ([20], [14]). These global response strategies presented myriad opportunities as well as challenges. Opportunities include expanded possibilities of identifying and exploiting new products, processes or markets through e-commerce [1].

Challenges came in the form of business constraints that made it necessary for small and medium-scale sector firms to turn to e-commerce to continue running their operations remotely ([19], [25]). In Kenya, for example, the Communications Authority [26] published an ICT sector statistics report for the period July to September 2020 that showed total data/Internet subscriptions increased by 4.8 percent to 43.4 million, while the value of customer-to-business digital money transfers increased by 64.8 percent during the period compared to the previous quarter, aimed at reducing cybercrime. The total utilized international bandwidth increased by 14.2% from 3,238.21 Gbps to 3,697.62 Gbps during the same time period [26].

Even though the adopted digital media solutions as mitigation to implications of the COVID-19 pandemic can enhance customer care services and targeted marketing due to the accumulation of big data, these also have unfortunately continued to attract integrity concerns due to cyberattacks ([26], [15], [16], [18], [27]). Cybercriminals have increased their attacks, especially on small and medium enterprise sector firms, for fraudulent gains, taking advantage of their inadequate experience with technology and lack of access to strategic resources such as finance and skilled staff ([16], [28], [15], [21]). Breach of data through cybercrime may not only expose organizations to legal suits from customers but may also negatively 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 ([15], [25]). Unfortunately, not much has been done to examine the impact that cyber security concerns continue to have on SME sector firms, especially in less developed countries ([11], [29], [23], [30], [31]). This is the premise upon which the current study was undertaken to establish cyber security concerns for selected medium-scale manufacturing enterprises in Kenya. The objective is to generate empirical data to drive policy programmes geared towards addressing cyber security concerns for firms, especially those in the SME sector, due to their unique challenges related to their small size.

3. Review of Theoretical and Empirical Literature

3.1. Theoretical Review

There is extant literature that seeks to explain the adoption of technological innovations by society [25]. According to diffusion innovation theory [32], adoption does not happen uniformly across society; rather, some people adopt an innovation earlier than others when they perceive an idea as innovative and useful. The innovative idea or product then gains momentum over time as it spreads through specific populations and communities [32]. Similar to diffusion innovation theory, the Unified theory of acceptance also seeks to explain user intention to adopt technology [33]. Similarly, the Resource Based View (RBV) model has also been applied to explain various phenomena, including information systems [34]. Peteraf [35] used the 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 capabilities to align technological innovations to a firm's strategic objectives rather than the adopted technology in itself. In a similar line of study, reference [36] identified conducive factors as one of the constructs that impact an individual's perception and user behaviour. However, Powell [37] noted that the emphasis of the investigation shifted from industry structure to the firm's internal structure, resources, and competencies. These theories present important challenges that have ramifications for SMEs' e-commerce adoption [25]. These theories are relevant to the current study because they can be used to understand better the manner and speed of digitization, including the decisions by SME sector firms to adopt e-commerce and related technology solutions in the wake of the COVID-19 pandemic.

3.2. Empirical Review

Empirical studies have been conducted seeking to investigate various aspects of e-commerce adoption and cyber security concerns in different parts of the world ([25], [17], [29], [23], [31], [39], [40]). In Kenya, reference [40] reported that the arrival of submarine fibre optic cable improved bandwidth availability, thus facilitating businesses to efficiently conduct businesses and deliver services through collaborative efforts across organizational, social and geographic boundaries. As a result of the operationalization of the fibre optic cable, many organizations in Kenya started taking advantage of the increased bandwidth and Information Communication Technology capabilities brought about by the fibre optic cable to conduct e-commerce [26]. According to reference [42], organizations adopt e-commerce to enhance customer interaction efficiency through online registration, content personalization and real-time online support. Effective deployment of digital sales and marketing capabilities leads to enhanced organizational financial performance [43].

Similarly, established a correlation between e-commerce capability allocation and the strong financial performance of a business enterprise. Though e-commerce solutions can improve service delivery to customers, the same continues to attract integrity concerns due to cyberattacks on organizations, including SME sector firms [17]. The situation became more pronounced with the advent of the novel coronavirus disease outbreak of 2019 that forced many SME sector firms to adopt digital sales and marketing channels to continue operating virtually, given movement restrictions ([14] [25]). In Kenya, the Communications Authority of Kenya (2021) sector statistics report for the July to September 2020 period reported a 152.9% increase in cyber-attacks, with 35.1 million incidents attributed to increased uptake of e-commerce in response to the COVID-19 pandemic.

Cybercrime is not a new phenomenon considering existing empirical literature on this matter ([23], [45], [29], [39], [17], [40], [18], [38]). According to reference, while most cybercrimes are carried out to make money for cybercriminals, other cyber-related attacks are carried out directly against computers or devices to damage or disable them or to spread malware, illegal information, images, or other materials. In the case of SMEs, cybercriminals have taken advantage of entrepreneurs' lack of technological competence and access to strategic resources such as financing to implement more secure information management systems ([16], [47]). According to reference [31], most businesses were aware of the necessity of information system security and the need to implement security measures as a result of their reliance on IT systems. Viruses, human errors, computer theft, and system and software faults were found to be the top issues facing information security system management [48], despite the ICT security measures in place. Financial fraud seems to feature strongly among reported occurrences, with loss of computer assets and systems user threat being a reoccurring problem among the organizations analyzed [31]. After conducting a study on a framework to guide information security measures for banking information systems in Kenya, reference [39] revealed a similar finding. According to the survey, the main barriers to successful cyber security in Kenya's banking business were a lack of proper communication, a competent workforce, and customer security awareness [39]. As a result, reference [48] study proposed that segregation of roles, physical security controls, and inventory of IT assets be implemented to improve cyber security. Despite earlier empirical results and recommendations, cybercrime continues to be a significant barrier to businesses and entrepreneurs seeking to maximize e-commerce ([17], [25], [18], [38]).

4. Materials and Methods

A descriptive research design was adopted in obtaining primary data from senior executives of enterprises from a cross-section of the manufacturing or value addition sector in Nairobi County, Kenya. The manufacturing sector was chosen not only because it is part of the big four agenda in Kenya but also because its output is often traded in local and international markets rather than service output. Nairobi County was picked as the study's geographical setting because over 80 per cent of manufacturing firms are based there, and this capital city is the regional business hub [12].

The senior executives in charge of strategic business units were identified as the unit of observation because they were judged to be in a better position to respond to items touching on cyber security concerns in their respective firms. The unit of analysis was all the one hundred and twenty (120) medium-scale manufacturing enterprises with an employment level of between fifty-one and two hundred employees, considering the definitions provided for in the MSE Act of 2012 [44].

The one hundred and twenty medium-scale manufacturing enterprises were identified per data obtained from the Kenya Association of Manufacturers [12] and Kenya Bureau of Statistics, and the licensing department of the Nairobi County Government. This identification exercise was done to ensure inclusion in the study of only legally compliant firms. Medium-scale manufacturing enterprises were chosen because most studies on firm performance have mainly examined micro, small or large-scale enterprises concerning governmental-industrial policies ([2], [4]). This implies a missing middle with inadequate empirical data and policy solutions that could consider the unique nature of challenges experienced by these types of firms [9]. This may counteract stakeholder efforts in designing programmes to facilitate best and aid the optimal performance of this sector.

The units of analysis were then divided into three groups based on their degree of employment: 51-100, 101-150, and 151-200. Food processing, woodworking, fabricated metal products, and leather, textiles, and garments were all separated into five (5) subcategories [9]. This was done to ensure the entire population was represented fairly and without bias [14]. This approach was deemed valuable since it would allow researchers to investigate specific sub-group features [9]. The mean responses on a Likert scale of 1–5 for each tested question were determined by adding up the codes from all the respondents.

5. Results and Discussion

5.1. Response Rate

The study recorded a 63.33% response rate, as presented in Table 1. This means that seventy-six (76) senior executives participated in the study out of the target population of one hundred and twenty (120) medium-scale manufacturing enterprises. The non-response may be due to a combination of factors, including time constraints on the part of the respondents.

Table 1. Response rate

Stratum	Employment Levels			Totals
	51 – 100	101 – 150	151 – 200	
Food Processing	7	5	3	**15**
Wood Workings	5	4	4	**13**
Fabricated Metal Products	8	5	4	**17**
Non-Metallic Products	5	5	4	**14**
Leather, Textiles & Garments	8	6	3	**17**
TOTALS	**33**	**25**	**18**	
%	**43.4**	**32.9**	**23.7**	**76**

Table 2. Items on cyber security concerns

Item Description	SD %	D %	NS %	A %	SA %	Mean Response
Digitization of our processes is a high priority for the enterprise	0	15.7	31.5	51.3	1.3	3.38
The enterprise has experienced a cyber security-related incident within the last one year.	0	0	32.9	67.1	0	3.67
The enterprise has well-documented policies for data security.	0	35.5	52.6	11.8	0	2.76
The management is conversant with the applicable data security laws in the country.	0	42.1	51.3	6.6	0	2.64
The enterprise has developed cyber risk maps showing current and emerging risks.	39.5	34.8	16.7	5.3	0	1.96
The enterprise has the right talent to lead cyber initiatives related to Information Communication Systems.	7.9	38.1	42.1	11.8	0	2.58
The data protection law in Kenya has had a positive effect on Cyber security and customer data protection.	0	51.3	39.5	9.2	0	2.58
The cyber incident response plan for the enterprise is tailored to rapidly contain damages and mobilize response resources if a cyber incident were to occur.	5.2	42.1	40.8	11.8	0	2.59
The enterprise has awareness programs tailored for high-risk employee groups handling information communication systems and connected products.	0	43.4	50.0	6.6	0	2.63
The cyber risk management program and capabilities are aligned with industry standards and peer organizations.	0	48.7	50.0	1.3	0	2.53
The enterprise allows third-party ad platforms and trackers on our websites.	0	0	39.5	60.5	0	3.61
The business has programmes to protect the firm against cyber risks attributable to members of staff and third parties.	2.6	43.4	44.7	9.2	0	2.61

SD- Strongly disagree; **D**-Disagree; **NS**-Not sure; **A**-Agree; **SA**-Strongly agree

As presented in Table 1, most of the respondents were from firms with an employment level of 51-100 (43.4%), followed by 101-150 (32.9%) and 151-200 (23.7%), respectively. The distribution of respondents in Table 1. assures a well-balanced sample since the responses were well distributed across the clusters in the target group.

The respondents were then asked to consider statements on cyber security and indicate the extent to which they agree or disagree regarding current activities in their respective enterprises. Table 2. presents mean responses received using a Likert scale of 1 – 5 for each tested item, calculated by summing up the codes from all the respondents.

Table 2. shows that 67% of the sampled enterprises have experienced a cyber-related incident within the last one year. Despite this, only about 6% of the executives indicated that they are conversant with the applicable data security laws in Kenya, while 50% of the respondents are unsure whether their enterprises' cyber risk management program and capabilities are aligned with industry standards.

When asked to indicate what the respondents consider the most common cyberattack threats for manufacturing firms in Kenya, theft of intellectual property was the most cited cyber security threat (38% of the sampled executives), followed by phishing (24%) and malware (22%), respectively. Five policy issues were proposed when asked what policies the government can put in place and/or what needs to change to address cyber security concerns for medium-scale manufacturing enterprises in Kenya. Five policy issues were proposed, as presented in Table 3.

Table 3. Proposals on policy initiatives

Item Description	f	%
Capacity building of entrepreneurs by the government	23	30.26
Closer collaboration between government and industry	18	23.68
Funding to enable address inherent weaknesses of SMEs	33	43.42
Government to avail secure ICT infrastructure for use by SME sector firms.	24	31.58
Government to invest in ICT investigation capabilities.	22	28.95

5.2. Discussion and Implications

This study sought to establish cyber security concerns for medium-scale manufacturing enterprises in Kenya. The study revealed that about 51% of the sampled firms had prioritized the digitization of processes for the enterprise. This finding seems to confirm observations from previous studies to the effect that digital platforms have now become the new frontier for local and international trade for SME sector firms, especially in a globalized business environment ([16], [17], [21], [30], [31], [38], [39]). The findings of this study are also in line with the Communications Authority of Kenya (2021) sector statistics report for the July to September 2020 period, which reported a 152.9 per cent increase in cyber-attacks with 35.1 million incidents attributed to increased uptake of e-commerce in response to the COVID-19 pandemic. SME sector firms have therefore invested in e-commerce solutions to remain competitive, especially in the aftermath of the coronavirus disease outbreak. This study also established that 67% of the enterprises had experienced a cyber-related incident within the last one year, with intellectual property being the most cited cyber security threat at 38%, followed by phishing (24%) and malware (22%). This means that Kenya is not immune to cybercrime similar to what has been reported elsewhere around the world ([18], [28], [17], [22], [29], [45]).

This study also revealed that only about 6% of the executives are conversant with the applicable data security laws in the country, while about 50% are unsure whether their enterprises' cyber risk management program and capabilities are aligned with industry standards. This finding which essentially means that there is an information, knowledge and skills gap in SME sector firms, is consistent with some studies reviewed in this study ([22], [23], [31], [3], [16], [25], [29], [9]), cybercrime continues to be a major challenge for entrepreneurs globally. Adoption of e-commerce solutions by SME sector firms, therefore, presents policy, legal and regulatory challenges, especially for regulatory agencies and entrepreneurs. For entrepreneurs, infiltration of information and communication systems by cyber criminals may not only expose SMEs to legal suits from customers. However, it may also affect their competitiveness by losing customer confidence due to violation of privacy, ransomware, eavesdropping, stolen business strategies and intellectual property. This negatively impacts not only SME sector firms regarded as an important step towards overall economic development but also other sectors of the economy, potentially leading to the possible shutdown of critical national infrastructure through cyber terrorism.

6. Conclusion and Recommendations

The study concluded that cybercrime is a global problem that has serious implications for organizations and business enterprises. There is a need, therefore, for public-private partnerships at the local and international levels for mutual benefit. Specifically, businesses should have a forum to share cyber intrusion and penetration incidences and methodologies, in addition to improving their current digital systems to identify key risks, vulnerabilities and critical information assets to form the basis for implementing controls and proactive management of information risks.

Given the important role played by SME sector firms in income generation and employment creation, the Kenyan government needs to come up with more specific legislative initiatives and policies geared towards facilitating businesses in the wake of constraints occasioned by the coronavirus disease outbreak. Policy initiatives should encourage and facilitate SME sector firms to have in place online security protocols requiring authorization of online transactions to be preceded by authentication to ensure that e-commerce and customer data is protected from disclosure or modification by unauthorized persons. The policy framework should also allow for a technology grants system to link Universities, Research and technology institutions with business enterprises. At an international level, there is a need for cooperation in the cyber security field by governments around the world to facilitate sharing of cybercrime-related intelligence, capacity building and formulation of legal frameworks to address cybercrime and cyber security. It would enhance contributions by e-commerce-compliant businesses towards global sustainable development.

Acknowledgements

We want to acknowledge all the respondents for availing themselves during the study. To all those who contributed in one way or another to actualizing this study and whom we may not individually mention by name, we highly appreciate your contributions.

References

[1] Alexander W. Bartik et al., "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, vol. 117, no. 30, pp. 17656-17666, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Gema Álvarez, and Ana I. Sinde-Cantorna, "Self-Employment and Job Satisfaction: An Empirical Analysis," *International Journal of Manpower*, vol. 35, no. 5, pp. 688–702, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[3] Barbara Bigliardi, Pierluigi Colacino, and Alberto Ivo Dormio, "Innovative Characteristics of Small and Medium Enterprises," *Journal of Technology Management and Innovation*, vol. 6, no. 6, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[4] Abor, J., and Peter Quartey, "Issues in SME Development in Ghana and South Africa," *International Research Journal of Finance and Economics*, vol. 39, pp. 218-228, 2010. [Google Scholar] [Publisher Link]

[5] International Monetary Fund, Economic Outlook Report, 2021. [Online]. Available: https://www.imf.org/en/publications/weo/issues/2021/01/26/2021-world-economic-outlook-update

[6] OECD, OECD Digital Economy Outlook 2020, OECD Publishing, 2019. [Online]. Available: http://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm

[7] X Kongmanila, and T Kimbara, "Corporate Financing and Performance of SMES: the Moderating Effects of Ownership Types and Management Styles," 2007. [Google Scholar]

[8] UNIDO, *Sustaining Employment Growth: the Role of Manufacturing and Structural Change*, Industrial Development Report, UNIDO, Vienna, 2013. [Google Scholar] [Publisher Link]

[9] Evans Mwasiaji, "The Effect of Government Policy on the Performance of Selected Manufacturing Enterprises in Kenya," *International Journal of Economics, Business and Management Research*, vol. 3, no. 12, pp. 198-210, 2019. [Google Scholar] [Publisher Link]

[10] Government of Kenya, Economic Survey 2020, Kenya National Bureau of Statistics. Nairobi, Kenya: Government Printer, 2020.

[11] Alice Nambiro Wechuli et al., "Cyber Security Assessment Framework: Case of Government Ministries in Kenya," *International Journal of Technology in Computer Science and Engineering*, vol. 1, no. 3, pp. 100-113, 2014. [Google Scholar] [Publisher Link]

[12] Kenya Manufacturers Association, Survey of the Manufacturing Sector in Kenya, Kenya Association of Manufacturers, Nairobi.

[13] Parliament Budget Office, 2020. [Online]. Available: http://www.parliament.go.ke/sites/default/files/2020-03/unpacking%20of%20bps%202020%20final.pdf

[14] Evans T. Mwasiaji, Ambrose O. Jagongo, and James O. Ogutu, "Coronavirus Disease Outbreak and the Supply Chain of Selected Small and Medium Manufacturing Enterprises in Kenya," *International Journal of Business and Social Science*, vol. 11, no. 4, pp. 7-16, 2020. [CrossRef] [Publisher Link]

[15] Tracy Tam, Asha Rao, and Joaane Hall, "The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath," *Digital Government: Research and Practice*, vol. 2, no. 2, pp. 1-8, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] H Laura, Small Businesses Drive China's Economy: the Coronavirus Outbreak Could be Fatal for Many, 2020. [Onlne]. Available: https://edition.cnn.com/2020/02/14/economy/coronavirus-china-economy-small-businesses/index.html

[17] Navid Ali Khan, Sarfraz Nawaz Brohi, and NZ Jhanjhi, "UAV's Applications Architecture Security Issues and Attack Scenarios: A Survey," *Intelligent Computing and Innovation on Data Science*, vol. 118, pp. 753-760, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Interpol, COVID-19 Cyberthreats, 2020. [Online]. Available: https://www.interpol.int/en/crimes/cybercrime/covid-19-cyberthreats

[19] GEM, Diagnosing COVID-19 Impacts on Entrepreneurship, Global Entrepreneurship Research Association, London Business School, Regents Park, London NW1 4SA, 2020.

[20] Peterson, P., Business Email Compromise (BEC): Coronavirus A Costly New Strain of Email Attack, 2020. [Online]. Available: https://www.agari.com/email-security-blog/business-emailcompromise-bec-coronavirus-covid-19/

[21] Ogoti Elijah Sokobe, "Factors Influencing Adoption of Electronic Payment By Small and Medium Hotel Enterprises in Kisii Town, Kisii County, Kenya," *International Journal of Novel Research in Computer Science and Software Engineering*, vol. 2, no. 2, pp. 5-18, 2015. [Google Scholar] [Publisher Link]

[22] Paula Musuva Kigen, "Kenya Cyber Security Report 2014, Rethinking Cybersecurity, An Integrated Approach: Processes, Intelligence and Monitoring," Nairobi: Serianu Limited, 2014. [Google Scholar] [Publisher Link]
[23] Liene Kreicberga, "*Internal Threat to Information Security Countermeasures and Human Factor Within SME,"* Kiruna: Lulea University of Technology, 2010. [Google Scholar] [Publisher Link]
[24] World Health Organization, Coronavirus Disease (COVID-19) Pandemic, Geneva, Switzerland, 2020. [Online]. Available: https://www.who.Int/Emergencies/Diseases/Novel-Coronavirus-2019
[25] Evans Mwasiaji, John M. Kandiri, and David M. Minja, "Policy Framework for Cyber Security Concerns and Performance of Small and Medium Enterprises for Global Economic Recovery amidst Covid-19," *The International Journal of Business Management and Technology*, vol. 5, no. 3, pp. 51-59, 2021. [Publisher Link]
[26] Communications Authority of Kenya, Cyber Threats on the Rise with Increased Reliance on ICTS in the Mitigation of COVID-19 Pandemic, 2021. [Online]. Available: https://ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic
[27] J. Longbottom, "Coronavirus Forces Businesses to Adapt to Survive the COVID-19 Pandemic," 2020. [Online]. Available: https://www.abc.net.au/news/2020-03-19/how-businesses-adapting-to-survive-covid-19-coronavirus/12068696
[28] Yolanda Redrup, Beverage Maker Lion Hit by Cyberattack. Finance, 2021. [Online]. Available: https://www.afr.com/technology/beverage-maker-lion-hit-by-cyber-attack-20200609-p550w3
[29] Mike Mcguire, and Samantha Dowling, Cyber-Crime: A Review of the Evidence Summary of Key Findings and Implications Home Office Research Report 75, Home Office, United Kingdom, 2013. [Google Scholar] [Publisher Link]
[30] Government of Kenya, Cyber Security Strategy, Ministry of Information Communications and Technology, Nairobi: Government Press, 2014.
[31] Makumbi E. A et al., "*An Analysis of Information Technology (IT) Security Practices: A Case Study of Kenyan Small and Medium Enterprises (SMES) in the Financial Sector*," Nairobi: University of Nairobi, 2012. [Google Scholar] [Publisher Link]
[32] G.A. Rogers Barnett, Mathematical Model of Diffusion Process, in a Viswanath & G.A. Barnett (HRSG.), The Diffusion of Innivations – A Communication Science Perspective (S. 103 – 122) New York: Peter Lang Publishing, 2011.
[33] Venkatesh Venkatesh, James Y.L. Thong, and Xin Xu, "Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead," *Journal of the Association for Information Systems*, vol. 17, no. 5, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[34] J.B Barney, and B Tyler, "The Prescriptive Limits and Potential for Applying Strategic Management Theory," *Managerial and Decision Economics*, in Press, 1991. [Google Scholar]
[35] Margaret A. Peteraf, "The Cornerstones of Competitive Advantage: A Resource-Based View," *Strategic Management Journal*, vol. 14, no. 3, pp. 179-192, 1993. [CrossRef] [Google Scholar] [Publisher Link]
[36] Venkatesh Venkatesh, "User Acceptance of Information Technology: Towards A Unified View," *MIS Quartely*, vol. 27, no. 3, pp. 425-478, 2003. [CrossRef] [Google Scholar] [Publisher Link]
[37] Thomas C. Powell, "Competitive Advantage: Logical and Philosophical Considerations," *Strategic Management Journal*, vol. 22, no. 9, pp. 875-888, 2001. [CrossRef] [Google Scholar] [Publisher Link]
[38] Sam Curry et al., "*Big Data Fuels Intelligence-Driven Security*," RSA Security Brief, 2013. [Publisher Link]
[39] Stella WanjiruNjiru, "*A Framework to Guide Information Security Initiatives for Banking Information Systems, Kenyan Banking Sector Case Study*," Nairobi 2013. [Google Scholar] [Publisher Link]
[40] Laureen Akumu Ndeda, and Collins Otieno Odoyo, "*Cyber Threats and Cyber Security in the Kenyan Business Context*," *Global Scientifc Journals*, vol. 7, no. 9, pp. 576-582, 2017. [Google Scholar] [Publisher Link]
[41] Government of Kenya, Kenya Vision 2030: Ministry of State for Planning, National Development and Vision 2030. Sessional Paper No. 10 of 2012. Nairobi: Government Printer, 2012.
[42] Kevin Zhu, "The Complementarity of Information Technology Infrastructure and E-Commerce Capability: A Resource Based Assessment of Their Business Value," *Journal of Management Information Systems*, vol. 21, no. 1, pp. 167-202, 2004. [CrossRef] [Google Scholar] [Publisher Link]
[43] Mahmood H Shah, Sajid Khan, and Mark Xu, "A Survey of Critical Success Factors in e-Banking," *European, Mediteranean and Middle Eastern Conference on Information Systems*, 2007. [Google Scholar] [Publisher Link]
[44] Government of Kenya, MSC Act 2012. Kenya Gazette Supplement 219(2013)(Acts No. 55), 2013. [Online]. Avilable: https://www.industrialization.go.ke/images/downloads/policies/micro-and-small-enterprises-no-55-of-2012.pdf
[45] Robin Gandhi et al., "Dimensions of Cyber-Attacks: Cultural, Social, Economic and Political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28-38, 2011. [CrossRef] [Google Scholar] [Publisher Link]
[46] KNBS, Economic Survey, Kenya National Bureau of Statistics, Nairobi, Government Printers, 2019.
[47] Ackerman Jr. R, The Cyber Skills Shortage Continues to Balloon-and Think Tanks Aren't Helping, 2019. [Online]. Available: https://www.rsaconference.com/industry-topics/blog/the-cyber-skills-shortage-continues-to-balloon-and-think-tanks-arent-helping
[48] A. Roy, Top Ten Security and Privacy Challenges for Big Data and Smartgrids, Fujitsu Laboratories of America.