Cybercrime, Cyber Security and the Economy: A Legal Perspective

Everlyn K. Maika

Abstract

In the recent past, Kenya has experienced exponential growth in its cyberspace. It is estimated that about 42% of the Kenyan population has access to the internet as at January 2022. Further, many institutions within the public and private sectors are now providing their services in the digital space through online platforms. This has created great opportunities for commerce as well as networking for individuals across the various social platforms. Thus, the Kenyan economy is now heavily reliant on technology. The rapid advancement within the cyberspace and use of technology has exacerbated vulnerabilities, threats and attacks in the cyberspace. This paper takes a two pronged approach to cyber security through legal and economic lenses by examining the extent of cybercrime and threats that have become a great challenge to the security of the cyberspace as well as its consequences. It also analyses the legal and policy framework for cyber security in the country. This research was conducted through a review of literature and data on the subject. The findings herein indicate that Kenya is experiencing high numbers of cybercrime, attacks and threats targeting institutions as well as individuals which has resulted in significant losses to the economy, institutions and individuals. The paper recommends adoption of cyber security measures to effectively mitigate the effects of these cyber threats and attacks.

Key words*: cyber-attacks, cybercrime, cyberspace, cyber security, digital economy, threats.*

Introduction

The Kenyan economy is projected to grow at the rate of 5.5% in 2022 and 5.2% in 2023 according to the World Bank projection (Mathenge, Ghauri, Mutie, Sienaert, & Umutesi, 2022). This growth will largely be contributed to by the steady growth of economic activities within the cyberspace. Kenya has experienced high levels of digitization and technological advancement resulting in improved service delivery within various sectors of the economy (Muthengi, 2015) leading to more Kenyans embracing digital technology for various aspects of life. A 2016 report by the Kenya National Bureau of Statistics shows that 39% of private enterprises are engaged in e-commerce. Similarly, the Kenya National Economic Survey Report 2022 shows that the value of the ICT sector expanded by 6.9% from Kshs. 522.5 billion in 2020 to Kshs. 529.8 billion in 2021.

Following this growth, government policies are focusing and incorporating digital infrastructure into the Kenyan society. This is evidenced by the prominence given to digital strategies within the various development agendas and plans. The government has unveiled policy documents envisaged to propel Kenya towards a prosperous digital economy. Key among these documents are the Kenya Digital Blueprint and the Kenya National Digital Master Plan 2022-2023. The Digital economy blueprint envisions a digitally empowered citizenry, living a digitally enabled society. The digital master plan on the other hand, aims at leveraging and deepening the contribution of ICT to accelerate economic growth. These documents acknowledge that emerging technologies have great potential for impact on economic development.

The Kenyan economic ecosystem is composed majorly of small and medium enterprises (SMEs) that form the backbone of the economy. These enterprises have embraced ICT in their operations aimed at improving their business efficiency and developing competitiveness. The digital space offers a number of advantages as well as a myriad of challenges inherent within the cyber space (Muhati, 2018; Okuku, Renaud, & Valeriano, 2015). While the cyberspace is full of opportunities and great potential for businesses and individuals, it also contains many risks, challenges and threats in equal measure. The degree of these

risks and threats is directly linked to the degree of growth in digitization. As such, the more the Kenyan society embraces ICT, the more the risks and threats grow (Kamary, 2018).

Small and Medium Enterprises (SMEs) are facing a lot of challenges some being cyber related. The cyber challenges include inadequate funds, limited technical knowledge and lack of proper awareness on cyber security among others (Muhati, 2018). According to Muhati (2018), these entities are worst hit by cyber threats and almost half of cyber-attacks in Kenya are targeted at SMEs (Hakmeh, 2017).

The review of literature on cyber security in Kenya shows that indeed there exists high levels of cyber threats and cybercrime targeting businesses and individuals. However, there is limited academic literature on the usefulness of cyber security in countering the effects of cybercrime on the economy within the Kenyan context. This paper therefore, looks at the role of cyber security strategies in countering cybercrime thus enhancing and fostering economic growth.

This paper seeks to contribute to the academic discourse on cyber security in Kenya by attempting to establish a link between cybersecurity and economic growth.

Theoretical Framework

There are a number of theories formulated around the subject of cyber security and ICT in general, this paper will be founded on the *Routine Theory* of cyber security. This paper focuses on cyber security through the lenses of cybercrime manifested in cyber-attacks and cyber threats targeted at businesses operating within the digital space. Thus, the study was inclined towards the criminal components and their effects within the subject of study herein.

The *Routine theory* assumes that criminals commit crime because they had the opportunity and victims may not have been victims if they took appropriate measures to protect themselves. It further posits that crime occurs when three elements converge; a potential offender, a suitable target and the absence of a capable guardian. That all the three elements must be present for a crime to be

actualized (Purpura, 2013). This theory is particularly useful in understanding the rate and trends in cyber threats, attacks and cybercrime generally. Turvey, argues that the lack of any of the three elements sufficiently prevents the actualization of a crime (Turvey, 2013). For purposes of this study, the three elements are cybercriminals, digital economy and cyber security respectively. This study relied on this argument and posits that robust cyber security can prevent the actualization of cybercrime. It further helps to illustrate why cybercrime is on the rise and why cyber security strategies are critical in dealing with it.

Methodology

This study was a qualitative analysis of primary and secondary sources of literature on the subject. Insights were drawn from studies, articles, reports, policies and legal instruments relating to the subject of study. The insights were employed in the arguments advanced on the need for cyber security strategies.

Discussions and analysis of Findings

This paper reviewed literature relating to cyber security and cybercrime in Kenya with a view to establish the extent of cybercrime and the effects of cybercrime on the economy and businesses, and the legal and policy framework for cybersecurity. The findings of the review are discussed within the subsections below.

Cybercrime

Cybercrime, as already highlighted, is a global phenomenon that has recently gained collective attention from states within the United Nations (UN). In 2019, the UN general assembly voted to initiate negotiations for a convention to address the problem of cybercrime and to counter the use of ICTs for criminal purposes. An Ad hoc committee was established under resolution 74/247 which has since February 2022 been undertaking negotiations towards this end (UNODC).

There is no single accepted definition of cybercrime with the most preferred and commonly used definition referring to cybercrime as any unlawful action perpetrated by the use of a computer and or against a computer, system, network, program or data that pose a threat to the security of a nation, organization,

enterprise or individual (Muthengi, 2015). Cybercrime is composed of two categories; cyber dependent crimes that can only be committed by the use of ICT such as denial of services attacks (DOD) and; cyber enabled crimes which are the traditional crimes scaled up or sophisticated by the use of ICT such as online fraud. It is worth noting that most crimes now have an element of cyber (Swiatkowska, 2020).

Cybercrime has been reported to be on the steady rise and various factors have been noted to be contributing to this phenomenon. The growing number of cyber-attacks throughout the world coupled with the massive financial losses bring to the fore the vulnerabilities that exist in the cyber space and the serious consequences of cyber-attacks on the economy.

Some of the factors accounting for the increasing rates of cybercrime include the anonymity of carrying out criminal acts within the cyber space and the resultant minimal chance of getting caught (Swiatkowska, 2020). The structure of the cyber space makes it conducive for criminal activity, the lack of a single central control structure means that any person can carry out any action whether lawful or unlawful with the possibility of not being caught (Muthengi, 2015). Criminals exploit this unstructured nature of the cyber space compounded by the anonymity it affords them. Further, cybercrime is considered to be low-cost crime with very high profits thereby making it quite lucrative. This is highlighted by statistics showing that cybercrime is the third paying criminal venture globally after drug and arms trafficking (CSIS, 2018). Cybercrime has increasingly taken an economic angle with most attacks being economically motivated. The intention of the criminals being to disrupt normal operations of businesses with a view to gain financially by exploiting existing vulnerabilities as well as using illegally obtained data (Kajwang, 2022). As such it is possible to draw a connection between cybercrime and the economy because the greatest motivation for cybercrime is economic gain for cyber criminals.

The prevalence of cybercrime can also be attributed to the fact that cybercrime is relatively easy to commit and cyber-attack tools are now easily available for purchase at relatively affordable costs within the dark web (Swiatkowska, 2020).

Furthermore, the capabilities of cyber criminals are growing exponentially with the impact of their attacks equally growing in severity.

Cybercrime takes many forms, there are many categories of illegal activities that are prevalent within the Kenyan cyber space. The years 2019 and 2020 noted an increase in attacks in all key sectors including financial services, government, manufacturing and insurance (Serianu, 2021).

Cybercrime targeted at financial institutions as well as digital financial services increased and are of particular concern noting that banks in Kenya are highly reliant on technology for most services which makes them targets of cyber criminals (Wechuli, Wabobwa, & Wasike, 2017)

Malware is one of the forms of cybercrime that have become prevalent in Kenya. According to the Communication Authority cyber security report for April 2022, a total of 37,012,510 malware attack attempts were detected by the National KE/CIRT for the period between January to March 2022 with these attacks particularly targeting financial institutions (Serianu, 2021). This threat is quite serious with potential to adversely affect financial institutions due to the rise in online banking services. Online transactions, mobile banking and mobile money transfer platforms are widely used in Kenya due to their convenience and ease of access as alternative banking systems. The use of mobile devices for banking while offering convenience present serious security risks (Wechuli, Wabobwa, & Wasike, 2017). Malware specifically targeting mobile banking applications have increasingly been developed and deployed noting that most Kenyans are connected to the internet through their mobile devices via telecommunication networks (Okuku, Renaud, & Valeriano, 2015; Wakoli, Ogara, & Liyala, 2020). The report also noted an increase in malware targeted at automated teller machines (ATM). These malware are deployed against ATM machines triggering errors in the said machines that are then manipulated remotely by cyber criminals.

Ransomware was also noted to be on the increase specifically targeted at the financial sector as well as other sectors. This were targeted at the identity management systems of these institutions. Ransomware is one of the most

destructive tools of cyber-attack with potential for serious financial impact. It is deployed to encrypt data in a victims system and thereafter the criminals demand for payments to be made for them to decrypt the data and restore access (Swiatkowska, 2020).

Another growing threat noted is deployment of rogue devices. Rogue devices are malicious devices that are intentionally compromised for purposes of attacking computers, systems and data within a network of interconnected devices (Serianu, 2021). These devices gain access and carry out attacks within the infiltrated system. Phishing related social engineering is also on the increase. Phishing involves soliciting of personal information perpetrated through emails or malicious websites or mobile applications. These attacks usually seem to be originating from genuine sources. Customers are targeted largely by these attacks to obtain personal information that grants criminals access to the customer's account (Okuku, Renaud, & Valeriano, 2015; Jarud, 2020).

Business email compromise (BEC) was also noted to be on the rise (Serianu, 2021). This is a type of scam that targets companies and organizations for financial gain. They involve fraudulent emails purporting to be genuine usually requesting for funds transfer or privileged data (Interpol, 2021).

Another category of attacks steadily rising is mobile money fraud. The use of mobile money in Kenya is widespread making it a target of criminals who have developed elaborate scams targeting vulnerabilities within the mobile money platforms as well as customers' security lapses (Ndeda, Odoyo, 2019). The increased use of smartphones that hold personal information makes mobile devices used within the mobile money networks lucrative to criminals as they can easily obtain personal information that they can use to carry out fraudulent transactions (Wechuli, Wabobwa, & Wasike, 2017). Mpesa has been a target of such fraudulent activities which led to Safaricom engaging in public awareness warning customers about possible fraudulent attacks and how to protect against such attacks.

Cybercrime, as has already been alluded to herein, is one of the highest paying criminal ventures coming in at third place globally. Conversely, it is very costly

for economies, organizations, businesses and individuals. There are varying estimates on the cost of cybercrime to the world economy. Some of the statistics estimate that the cost of cybercrime to the global economy in 2022 is $7 trillion that is projected to rise to $ 10.5 by 2025 (Cybercrime magazine, 2022). Another estimate puts the cost at $600 billion which gives a percentage of 0.8% of the global GDP (CSIS, 2018). Regionally, cybercrime is estimated to have cost the African GDP $ 412 billion in 2021 which caused a reduction of more than 10%. Closer home, it is estimated that the Kenyan economy lost around $ 36 million to cybercrime (Interpol, 2021) which is a high cost for a developing economy.

These losses are costly for businesses and are even more detrimental to SMEs which are less resilient as they do not have huge budgets to invest in cyber security measures (Hakmeh, 2017). The effects on these business which make up the majority of the businesses in the country's digital economy have a direct negative impact on the economy.

The Human factor in cyber security

Most ICT devices, systems and programs are used, controlled and managed by human beings with the exception of some fully automated programs. This means that people are critical to the effective use of ICT and consequently have a role within the cyber security discourse. People can either be an enabler of cyber security or vulnerabilities (Okuku, Renaud, Valeriano, 2015).

According to the report by Serianu, there was an increase in attacks in 2020 from unsecured connections by people working remotely during the COVID-19 pandemic. This points to the human factor as one of the reasons for the increase in cyber-attacks. It has also been argued that cyber security measures and strategies should have the human factor as a central part and institutions should develop a cyber security culture which envisages how people interact with ICT systems (Njoroge, 2014). Cyber security should also focus on the role of humans who interact with ICTs. Users can be a serious threat to cyber security if they are not well informed of cyber security practices. These people need awareness on how to protect themselves in the cyberspace and general cyber hygiene (Okuku, Renaud, & Valeriano, 2015).

The study paper on human centered cyber security by KICTANet found that most cyber breaches in companies are as a result of human error as many citizens lack awareness on cyber-attacks. Thus, cyber security measures should not ignore the critical role of human beings. It should also address the needs of the people as well as the state's security concerns.

The importance of cyber security

Cyber security is concerned with the confidentiality, integrity and availability of information systems and data from malicious attacks (Ndeda, Odoyo, 2019). The International Telecommunications Union (ITU) defines cyber security as the collection of tools, policies, security concepts, security safeguards, guidelines, risk mitigation approaches, actions, training, best practices, assurances and technologies that can be used to secure the cyber environment and organizations and user's assets (ITU, 2018). In simple terms, it is interested in securing and protecting citizens and organizations which goes into the core of national and economic security that ultimately fosters and promotes human security.

Kenya has experienced a significant increase in coordinated attacks targeted at various sectors which have also been replicated across the region in East Africa (Serianu, 2020). This indicates that cyber-attacks in the region have taken a coordinated character that is linked to and similar to organized crime. The total cyber threats more than doubled from 139.9 million in 2020 to 339.1 million in 2021 (National Economic Survey, 2022; Serianu, 2020; Kshetri, 2016). These figures are quite staggering and clearly reflect the magnitude of the overall problem and the extent of the threats that are lurking in the cyberspace. Cybercrime and threats expose businesses negatively in various ways key among them being financial and data exposure that potentially have damaging effects on businesses (Ndeda, Odoyo, 2019).

These challenges are not unique to Kenya as they are prevalent around the world, thus making cyber security a very critical subject within any discussion or agenda on ICT and digital space. Cyber security is no longer frivolous, it requires attention from all sectors as well as individuals. Every sphere of human society is encountering the scourge of cybercrime and threats on a daily basis (Muhati, 2018)

This brings into sharp focus the centrality and indeed critical place of cyber security in society today. Society, but more importantly businesses cannot survive and grow without appropriate cyber security measures. There are emerging cyber security issues that have serious economic, social and political implications (Kshetri, 2016). Kshetri (2016) argues that there have not been scholarly studies on factors associated with cyber security in developing countries. He further posits that there have been efforts to close the economic gap in relation to factors contributing to digitization, there are lags in factors related to cyber security. These gaps create challenges that include ineffective approaches to cyber security and cybercrime. These factors increase the possibility of African businesses being excluded from the cyber space. This argument highlights the importance of developing appropriate cyber security that protects businesses and fosters the growth of the economy.

It is clear that the digital economy presents great potential for the country's economic prosperity as it can be harnessed for sustainable economic growth. This is achievable only if appropriate security measures are formulated to guard against the volatile nature of the cyberspace and the possible serious ramifications of potential attacks. Cyber security regulations and infrastructure are therefore critical to the development of the digital economy (Dahlman, Mealy, & Werlmelinger, 2016).

The achievement of full proof cyber security is impossible for various reasons including the highly dynamic nature of the cyber space as well as the constant growth in sophisticated technologies (Hakmeh, 2017). However, appropriate levels of cyber security and resilience can be achieved through the formulation of relevant legal instruments, policies, guidelines, safeguards, training and awareness.

Legal, Regulatory and Policy Framework

The growing rates of cybercrime have had serious ramifications for the economy estimated to have lost about $36 million to cybercrime (Interpol Africa, 2021). Like many countries around the world, Kenya has formulated domestic legal, regulatory and policy documents to address the challenge of cybercrime and cyber security. The country's approach to cyber security is also influenced by

international and regional frameworks that include the Council of Europe Convention on Cybercrime (Budapest convention) and the African Union Convention on Cyber security and personal data protection (Malabo convention). Therefore, cyber security within the Kenyan cyber ecosystem is grounded on the legal, regulatory and policy instruments discussed in the forthcoming section.

Legal and Policy Framework

Kenya has developed a number of laws, policies and strategies relating to cyber security. They include Computer Misuse and Cybercrime Act, Kenya Information Communication Act, Data Protection Act, Digital Economy blueprint, National Digital Master Plan and the National Cyber Security Strategy among others.

a) Computer Misuse and Cybercrimes Act

The main objective of this legislation is to protect the confidentiality, integrity and availability of computer systems, programs and data as well as facilitating the prevention, detection, investigation, prosecution and punishment of cybercrime. It also establishes the National computer and cybercrime coordination committee with the mandate of coordinating all matters relating to the cyberspace and cyber security in Kenya. The Act gives the committee the responsibility of ensuring the protection of critical infrastructure and developing a cyber-security framework for the country. It is further mandated to undertake international cooperation on all matters relating to cybercrime and cyber security. The Act also establishes offences relating to computers, systems, networks and data. The committee has developed the National cyber security strategy to streamline all activities relating to cyber security.

b) Kenya Information Communication Act

This Act establishes the Communication Authority of Kenya as the regulator for entities dealing in telecommunication and ICT in the country. The CA established the Kenya computer incident response team KE/CITR which is multi agency association framework responsible for national harmonization of cyber security reporting and incidence response. The Act also provides for the Commission's functions and responsibility in relation to cyber security.

Policy Framework

The following policy documents underpin and guide the efforts within the country on cyber security. They are aimed at ensuring a wholesome approach to the security of citizens, institutions and businesses through the protection of systems, networks, devices while maintaining and ensuring their confidentiality, integrity and availability.

a) Digital Economy Blueprint 2022–2032

The digital economy blueprint provides a framework for the country in the journey towards a sustainable digital economy. The blueprint envisions a digitally empowered citizenry living in a digitally enabled society. It is based on the realization that society must adapt to the reality of the place of digital technologies in the modern world.

The blueprint defines the digital economy as the entirety of sectors that operate using digitally enabled communications and networks leveraging internet, mobile and other technologies irrespective of industry. It is aimed to offer an opportunity to the country to join nations in the first world and contribute to the global economy. The framework is anchored on five pillars that underpin technology as the bedrock of Kenya's economic growth. These are digital government, digital business, infrastructure, innovation driven entrepreneurship and digital skills and values.

This framework further identifies cyber security as one of the key enablers for the digital economy noting that the protection and security of the integrity of electronic and digital systems is a paramount concern in a digitally enabled economy. Without robust cyber security policies and strategies, the digital economy will not be sustainable or successful. Therefore, one of the aims of the blueprint is to foster confidence, trust and security of the digital space.

It acknowledges that the lack of an effective cyber security mechanism will have a negative impact on the digital economy with potential loss of competitive ability and future economic strength.

b) Kenya National Digital Master Plan 2022-2023

The National digital master plan builds on the pillars of the Digital economy blueprint. The main objective of the master plan is the provision of quality, accessible, affordable, reliable, quality and secure information communication technologies in government aimed at positioning Kenya as a globally competitive digital economy.

It is similarly anchored on four key pillars; digital infrastructure, digital skills, digital innovation, digital enterprise and digital business. These pillars will guide in the provision of digital services to the citizens of Kenya, businesses and other stakeholders. It gives prominence to information communication technology as a key enabler in economic development of the country under vision 2030 and the digital economy.

Under the master plan, data protection and cyber management have been highlighted as key themes that cut across all the four pillars highlighting the need to secure the digital space and assets so as to maintain the confidence of citizens and businesses.

c) Kenya National Cyber Security Strategy 2022-2027

The Kenya National cyber security strategy is the country's key policy for cyber security. It was developed pursuant to the provisions of the Computer Misuse and Cybercrimes Act by the National computer and cybercrimes coordination committee (NC4). It is a frame work that seeks to provide for the implementation of cyber security measures in the country and address new challenges and emerging threats. It outlines the country's cyber security goals which include building a secure and resilient cyberspace and ensuring a safe and trusted cyberspace for the people of Kenya. The framework was formulated taking a whole of government approach on matters cyber security.

It is anchored on thematic pillars for effective cyber security for the public and private sector. The foundational pillars of the strategy are; cyber security governance; cyber security laws, regulations and standards; critical information infrastructure protection, cyber security capability and capacity building; cyber risks and cybercrimes management; cooperation and collaboration.

The legal and policy frameworks discussed herein have been formulated for the protection of systems, networks, devices while maintaining and ensuring their confidentiality, integrity and availability. The need for this protection is founded on notions of national security and the need to ensure security of citizens in all spheres of society. They are also developed taking cognizance of the fact that no single institution has the ability and capacity to deal with cyber security on its own. The frameworks establish coordinated mechanisms and approaches to cyber security. Further, the exponential growth in the digital front has necessitated inclusion of cyber security as a key component of national security. Throughout the world, countries that have advanced digital economies need to proactively engage in robust cyber security (Kovasc, 2018).

The frameworks further help to create clarity on the roles of different stakeholders within the cyber security ecosystem. They also shape the national security agenda as well as identifying and providing for appropriate allocation of resources (Kovasc, 2018).

Conclusion

This paper takes a two pronged approach to cyber security through legal and economic lenses by examining the extent of cybercrime and cyber threats that have become a great challenge to the security of the cyberspace as well as examining the consequences of cybercrime on businesses and the economy. It also analyses the legal and policy framework for cyber security in the country. In this quest, a review of literature, legal and policy instruments was undertaken.

The review of the legal and policy framework indicates that Kenya has made great strides in the formulation of laws, policies and strategies to protect the interests of Kenyans within the cyberspace. Indeed some of the laws, policy and strategy documents have adopted international best practices on cyber security. Further review of the policies indicates that Kenya has great aspirations of joining the developed economies of the world by embracing the digital economy that has merged the economic and social spheres of life noting that social platforms are now used for commercial purposes (Schwab, 2016).

A review of the available literature on the subject highlighted the critical place of the digital economy on the overall development of the country's economy as the digital economy presents great potential for organizations, businesses and individuals. It was noted that the Kenyan economy is on a large scale composed of SMEs that have been touted as the engine of economic growth.

The study also found that organizations, businesses and individuals continue to face an increasing level of cybercrime, risks, threats and attacks. It was noted that cybercrime is the foremost challenge facing businesses and individuals in the cyberspace in Kenya (Muhati, 2018). Indeed the statistics from the Communication Authority and Serianu indicate a spike in cyber-attacks within the last two years. This increase was attributed to various factors and vulnerabilities including the fact that cybercrime affords anonymity to criminals, availability of cyber tools for carrying out attacks and the vulnerabilities brought about by human beings as users of ICTs (Okuku, Renaud, & Valeriano, 2015; Swiatkowska, 2020).

For Kenya to realize the ambitious aspirations of joining the league of developed economies of the world as envisaged in the digital economy blueprint, harnessing the potential of the digital economy is crucial. As has already been highlighted, this can only be achieved by ensuring security of the digital economy through robust cyber security measures. While the country has formulated laws, policies and strategies on cyber security, the statistics on the trends and staggering levels of cybercrime indicate that the efforts so far have had minimal effect and that there is urgent need for increased efforts on cyber security.

The literature review also found that there is limited academic and empirical data on the relationship between cyber security and economic growth. The literature reviewed identified cybercrime as a serious challenge facing businesses in the cyberspace with serious financial implications on businesses and the economy. However, there is limited data that identifies the role if any that cyber security plays in connection to the mitigating the effects of cybercrime on the economy.

Recommendations

Following the review of literature, the paper makes the following recommendations;

- There is need for concerted efforts to be made by all relevant stakeholders to address the scourge of cybercrime that has been demonstrated as a serious challenge for the digital economy. Studies should also be conducted to identify the reasons for the prevalence of cybercrime within the Kenyan context with the aim of identifying possible tailored responses to the same. Counter measures need to be developed to protect the economy and SMEs from the debilitating effects of this problem.

- The paper also proposes training and awareness for businesses on the need to exercise due diligence and proper care in the cyber space to eliminate the vulnerabilities relating to the human factor. Businesses need to develop and inculcate proper cyber security culture within their operations to strengthen their business operations within the cyberspace. This will need adequate investment in training of staff and acquiring appropriate tools to protect against threats.

- It also proposes that SMEs need to invest in cyber security. As noted earlier on in this paper, almost half of cyber-attacks are targeted at SMEs which have been highlighted to be lagging in efforts to address cyber security challenges for various reasons.

- The paper also proposes that there is need for more research and studies to be carried out to establish the nexus between cyber security and economic development. As already highlighted herein, there is limited literature and data available on this subject. This limitation creates a gap in the body of knowledge on cyber security. This knowledge will be useful for policy makers and businesses in making decisions relating to cyber security and operations

References

A study paper on human-centered cyber security: Kenyan Fintech Sector.

African Union Convention on Cyber Security and Personal Data Protection.

Cate. F.H, Kuner. C, Svantesson.D, Lynskey. O, Millard. C. (2017). The rise of cybersecurity and its impact on data protection. *International Data Privacy Law, 7(2)*. https://www.repository:law.indiana.edu/facpub/2633

Communication Authority of Kenya cyber security Report, April 2022.

Computer Misuse and Cybercrime Act.

Cyber security Report. Cybercrime magazine (2022). https://cybersecurityventures.com/boardroom-cybersecurity-report

Cyber security as an economic enabler. (2016). ENISA.

Data Protection Act.

Economic impact of cybercrime. (2018). Center for Strategic and International Studies. https://www.csis.org/analysis/economic-impact-cybercrime

European Union Convention on Cybercrime.

General Data Protection Regulation.

Hakmeh. J. (2017). Cybercrime and the digital economy in the GCC Countries. Research paper, Chatham House.

Interpol Africa Cyber threat Assessment Report 2021.

Jarud U. (2020). Rogue devices mitigation in the IOT: A blockchain-based access control approach. https://researchgate.net/publication

Kamary. J. R. (2018). Cyber technology and insecurity in Africa. Thesis University of Nairobi.

Kenya Digital Blueprint.

Kenya Information Communication Act.

Kenya National Economic Survey Report 2022.

Kenya National Digital Master Plan.

Kenya National Cyber security Strategy.

Khanduja. V, Rawal R. (2017). Effects of cybercrime on economic development. *International Journal for Scientific Research & Development, 5(10)* https://www.academia.edu/35566431/Effect_of_Cyber_Crime_on_Economical_Development

Kajwang. B. (2022). Effect of cyber security risk management practices on performance of insurance sector: A review of literature. *International Journal of Research in Business and Social Science, 11(6)*, 334-340.

Kshetri N. (2016). Cyber security and development. *Markets, Globalization & Development Review*, 1(2). https://digitalcommons.uri.edu/mdgr/vol1/1552/3.

Kovacs, L. (2018). National Cyber security as the cornerstone of national security. *Land Forces Academy Review*, 23(2), 113-220.

Magutu P.O, Ondimu. G. M, Ipu. C.J. (2011). Effects of cybercrime on state security: Types, impacts and mitigations with the fiber optic deployment in Kenya. *Journal of Information Assurance & Cyber security.*

Mathenge, N.M, Ghauri, T.A, Mutie, C.K, Siernaert, A, Umutesi, A. (2022). Kenya Economic update:Aiming high-securing education to sustain the recovery https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099430006062288934/p17496106873620ce0a9f1073727d1c7d56.

Muhati. E. (2018). Factors affecting cyber security in Kenya: A case of small and medium enterprises. Strathmore University Thesis. http://su-plus.strathmore.edu/handle/11071/6013

Muthengi. F.M. (2015). On combating current and emerging cybercrimes in Kenya. *International Journal of Education and Research, 3(11).*

Mwania. K. (2016). Cyber threats and cyber security in ISO certified organizations in Kenya. Thesis University of Nairobi.

Ndeda L.A, Odoyo C.O. (2019). Cyber threats and cyber security in the Kenyan business context. *Global Scientific Journals, 7(9).*

Ngare. B. 2018. Factors contributing to cyber security framework in Kenya; A case study of Kenyan telecommunication companies. *Global Scientific Journal*, *6 (3)* www.globalscientificjournal.com

Njoroge. G. (2014). Human factors affecting favourable cyber security culture: A case of small and medium sized enterprises providing enterprise wide information systems solutions in Nairobi City County in Kenya. Thesis, University of Nairobi.

Okuku. A., Renaud. K, Valeriano. B. (2015). Cybersecurity strategy role in raising Kenyan Awareness of mobile security threats. *Information & Security: An internal Journal*, *32*.

Privacy and cyber security: Emphasizing privacy protection in cyber security activities. Report of the Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/cs_201412/

Purpura. P. (2013). Foundations of security and Loss prevention. Security & Loss prevention. 6th edition.

Ralarala. S. (2020).The impact of cybercrime on e-commerce and regulation in Kenya, South Africa and the United Kingdom. Thesis Strathmore University. https://su-plus.strathmore.edu/bitstream/handle/11071/10203

Serianu Africa Cyber security Report-Kenya 2019/2020.

Swiatkowska. J. (2020). Tackling cybercrime to unleash developing countries digital potential. Pathways for posterity commission background paper series; no.33 Oxford, United Kingdom.

The fourth industrial revolution. (2016) World Economic Forum https://www.weforum.org/focus/fourth-industrial-revolution

Turvey. B, Freeman. J. (2014). Forensic Victimology. 2nd edition.

Wakoli. L, Ogara. S, Liyala. S. (2020). An understanding of the cyber security threats and vulnerabilities landscape: A case of Banks in Kenya. *International Journal of Innovative Research and Advanced Studies*, *7(6)*.

Wechuli. N.A, Wabobwa. F, Wasike. J. (2017). Cyber security challenges to mobile banking in SACCOS in Kenya. *International Journal of Computer*, *27 (1)*, 133-140.