Role Of Public-Private Sector Partnerships In Mitigating Cyber Security Threats In Kenya.

By

Fred Jonyo and Kaudo Philip

Abstract

Increasing espionage, and technology-related crimes such as hacking have made cybersecurity a national priority in government and private sectors. Given the increasing vulnerabilities in cyber security and frequent attacks on both personal information and the realization that data protection and management is a shared responsibility, public-private partnerships in cybersecurity have been considered a viable approach to mitigating cybersecurity threats. This study therefore focused on assessing the role of public-private sector partnerships in mitigating cyber security threats. The study adopted both primary and secondary data in data collection. 15 key informants, purposively sampled will be involved in the study and their findings will be corroborated by the already existing literature that assesses the role of public-private sector partnerships on cybersecurity. The research found that addressing cyber security threats is a collective and shared responsibility that requires the partnership of both the private and public sectors. The study established that critical cyber issues including trust deficits, failure to standardize cyber policies and laws, and privacy concerns among others, continue to hinder public-private partnerships on cybersecurity. The study also found that public-private partnerships present viable opportunities for information sharing, innovation, and the development of effective regulatory frameworks to limit cyber-attacks. The research recommends development of effective and efficient systems of data sharing, cyber security inter-agencies and critical infrastructure protection. Other recommendations include conducting periodic joint audits and assessments, joint pooling of resources, joint training and sensitization on cyber security, establishment of a joint effective incident response and emergency management unit, strengthening frameworks and laws on cyber security and lastly further research is critical for cyber security.

Key Words: *Cyber Awareness, Cyber Security, Cyber Threats, Private Sector, Public Sector.*

Introduction

In the contemporary world which is characterized by internet technology, cybersecurity is emerging as a major concern. This is prompted by the fact that it has major implications for the state's national security, individual human rights and civil liberties, especially the rights to privacy and confidentiality and international legal frameworks. Globally, states and non-state actors continue to face cyber-security threats in the form of hacking and other forms, which have resulted in serious reputational and economic damages including phishing of critical information. For instance, in 2017, according to the USA Intelligence Community's World Wide Threat Assessment, cyber threats were considered as one of the greatest threats to global security. This has been manifested by the increasing rates of countries and private entities' networks being shut down, trade secrets being stolen, and even invasion of privacy of individuals and families, (US, 2017).

According to the Communication Authority of Kenya report published in October 2023, Kenya had witnessed a total of 860 million cyber security threats in the year 2022-2023 financial year. The report acknowledged that of the 860 million cyber security threats, 79% were a result of cyber criminals exploiting vulnerabilities and flaws in organizations' internal controls, system procedures, and information systems which they relied on to gain unauthorized access to critical organizational and personal information. Noteworthy, malicious software only accounted for 14% of the attacks while Distributed Denial of Services (DDOS) accounted for 6.5% of attacks, and attacks on web applications were also reported. The report noted that there is an increasing trend for cyber-attacks in Kenya, with the country experiencing more than 860 million cyber-attacks annually, against the 7.7 million annual attacks reported six years ago, (CAK, 2017).

In July 2023, Kenya suffered a high-profile cyber-attack that jeopardized the operations of government services including the e-citizen platform, and paralyzed access to more than 5000 government services. The attack was conducted by hackers who identified themselves as "Anonymous Sudan". Whereas the government held the view that no data was lost, the incident paralyzed government operations, (CAK, 2017). Subsequently, in July 2023, Microsoft released a report, notifying that a group of hackers had gained access to organizational email accounts of more than 25 organizations and government agencies.

Given the increasing trends in cyber security attacks, there is heightened focus, exemplified by establishing cyber security strategies and specialized cyber security agencies as mechanisms for mitigating the risks of cyber-security attacks. For instance, the North Atlantic Treaty Organization has already designated cybercrime as an official domain of warfare and warned member states against having vulnerable information system technologies that can be easily hacked. China on the other hand developed a cyber security law that prohibits any form of cyber space attack. The United

States also considered cyber security threats as key national security threats, (US, 2017).

Given the strong agreement that cyber security risk is a “shared risk”, there is a growing need for the involvement of private sectors and individuals in managing cyber threats. The private sector is viewed as a critical actor in cyber governance. It becomes very disadantageoue when the private sector isolates itself from this partnership, Etzioni, (2014). As a result of this, most cyber security strategies, developed by governments have largely focused on the private sector. In the United Kingdom and the United States of America, public-private sector partnership has been considered as the cornerstone of cyber-security strategy. The public-private partnership in cyber security is viewed as a strategic approach to ensure inclusivity against fighting all forms of cyber threats.

The government of Kenya, owing to the centrality of cyber security in national security has developed several cybersecurity policies, strategies, and frameworks in an attempt to counter the menace. Based on the fact that the government of Kenya considers the ICT sector a key and instrumental contributor to the achievement of Vision 2030 and envisions transforming Kenya into a digital economy, the government on 5th August 2022 launched the National Cybersecurity Strategy, that draws a practicable roadmap for addressing new challenges and dynamics of cyber security, (NC4, 2022).

Whereas there has been a growing need for the integration of public-private partnerships as a mechanism for addressing cybersecurity challenges, this step has been frustrated by the prevalence of several systemic and technological issues. According to O'Halloran, (2017), limited trust between the government and the private sector on information sharing remains a major issue in public-private partnerships. This is reiterated by the arguments put forth by Tropina and Callanan, (2015), who argued that though cyber security is a shared concern, the state cannot blindly trust private actors to fulfill critical infrastructure protection obligations voluntarily. O'Halloran, (2017) argues that limited trust between the public and the private sector on cyber security issues has degenerated into information-sharing issues. The other critical issue that impedes effective cybersecurity collaboration is the question about obligations regarding the exposure and disclosure of important cyber information that can facilitate the identification of threats and vulnerabilities of the cyber system. This is exemplified by the fact that many organizations are reluctant to share their security vulnerabilities for fear of facing civil litigation and regulatory scrutiny. For instance, most private entities are quite reluctant to partner or contact the public sector for help in addressing a cybersecurity threat, for fear of reprisals including information leaking to the general public. Furthermore, regulatory gaps also impede the development of public-private partnerships.

As O'Halloran, (2017) observes that cyber security is an international threat whose effect is felt both locally and internationally. The researcher argued that across the globe, one of the systemic issues lies in the fact there exists diverse differences in law and policies that guide cyber security across borders. These differences in law and policy are manifested in the differences in the capacities, roles, and reach of governments on cybersecurity, legal and policy limits on self-help by organizations, laws governing how evidence on cyber threats are to be gathered and used, parameters and perceptions of privacy among other issues. These critical systemic issues on policies and laws continue to impact how the private sector and the public sector should respond both unilaterally and collaboratively to cyber threats. This is necessitated by the fact that there is a significant lack of clarity regarding the legal and policy parameters of public-private cooperation, which frustrates the mitigation of cyber threats across borders.

Subsequently, the conflicting laws and policies on cybersecurity across borders, continue to hinder cross-border data transfer activities, aimed at investigating or assessing the vulnerabilities of diverse systems. The jurisdictional scope of the different data privacy laws and the consequences that private companies are likely to face if they breach the privacy obligations have also limited public-private cooperation in so far as cyber security is concerned. As Carr (2016) observed, there exists a serious disjuncture of expectations from both the private sector and public sector on cyber security. For instance, whereas the public sector (government) regards the private sector as a key actor in cybersecurity, the government remains reluctant to grant the private sector the mandate to oversee network security. Conversely, the private sector is not willing or inclined to accept liability for national cyber security or even share their system vulnerabilities with the public sector.

Given the emergence of technological and systemic issues on cybersecurity partnerships including limited trust among cyber security actors, differing interpretations of cyber security laws and privacy rights among different states and organizations, lack of clarity on the parameters of public-private cooperation, and the issues of exposure and disclosure among others, this study aims to fill this research gap, by assessing the critical role of public-private partnerships, putting into considerations the critical issues that hinder public-private partnerships.

Noteworthy, despite the growing government commitment to prioritize cyber security, including developing partnerships with the private sector and individuals, cyber security attacks and risks remain pertinent. As a result, there is a critical need to outline the role of public-private sector partnerships in cyber security and highlight some of the gaps that need to be mitigated to limit cyber threats.

Purpose and Objective of the Study

The focus of this study is to assess the role of public-private sector partnerships in mitigating cyber security threats. The study is therefore guided by this research question; what is the role of public-private sector partnerships in addressing cyber security threats?

Literature Review

According to Carr (2016), cyber-security is a multifaceted concept that refers to the integrity of individuals' personal privacy online, electronic commerce, security of critical information infrastructure, military threats and the protection of intellectual property. Cybersecurity therefore is protection against any unauthorized access to critical information of individuals and entities. Carr (2016), the state has largely been viewed as the main actor in the provision of national security including the protection of cyberspace and national borders. However, new dynamics in security, including the rise of global terrorism, cybercrime, and transnational crime among others have necessitated the involvement of the private sector as a co-actor of the state in handling cyber threats. Therefore, the partnership of the public-private entities on crime has been propelled by the assumption that mitigating cyber threats requires a collective responsibility and a shared mission. This collaboration should focus on information sharing and expertise sharing, aimed at managing cyber-related threats including cyberbullying and hacking.

Public-private partnerships have several benefits for both the public and private sectors. For instance, both parties benefit from sharing expertise, resources, knowledge, and best practices to make cyberspace much safer and resilient and to enhance customer satisfaction in the use of information infrastructure. According to Carr (2016), the public sector is most likely to benefit from the resources of the private sector like in technology and innovation. On the other hand, the private sector could also gain from public sector in financial budgets and also aid in developing national legislation including policies, strategies, and laws that are geared towards cyber security.

Van and Easton, (2021), public-private partnership fosters innovation and knowledge creation, which is key to finding solutions to network or system vulnerabilities that necessitate cyber threats. Their study also noted that the partnership between the public and the private sector involves closer relationships and interactions, manifested in the form of information sharing and knowledge sharing aimed at mitigating the gaps that expose systems to cyber attacks. This will be very critical in addressing the trust and confidence deficit, which stands out as a major challenge in cyber security, especially between the public and the private actors. Their findings corroborated the results of Carr, (2016).

Cyber forensics in smart cities require partnerships with both the private sector and the public sector, (Rao & Thatikonda, 2023). The resaerchers concluded their study by summaring the role of public-private sector partnerships so as to provide opportunities and platforms for sharing resources, knowledge, and expertise and complement the capacities of both the private and the public sectors. Further, they argued that the public-private partnership can result in the development of workable and agreeable regulatory frameworks that guide cyber security processes and also foster the building of public trust that is necessary for effective cyber forensics, (Rao & Thatikonda, 2023).

Juma, Arman and Hidayat, (2023), noted that public-private sector partnerships are very critical for fostering cyber security culture that encourages every actor to prioritize cyber security and also developing information-sharing channels on cyber threats. The researchers also noted that in cyber security, governments are the main protectors and regulators of cyber systems. As a result, collaboration between the public sector and the private sector is of essence because it helps fill the gaps including resource gaps, enforcement hurdles, and expertise challenges among others, that the public sector faces, (Juma, Arman & Hidayat, 2023).

Methodology

The study adopts mixed research methodologies including the use of questionnaires and interview guides. This integrates 15 purposively sampled respondents and analysis of documents that explore the discussion on public-private partnerships. The secondary data is collaborated with primary data which is obtained through in-depth interviews with cybersecurity. The respondents were drawn from both public and private sectors, while cognizance of the emerging issues on cybersecurity shared their expert knowledge on the opportunities for public-private partnerships in cybersecurity. The measurable variables involved were; information sharing, innovation, sensitization, and awareness creation, data sharing and development of cyber security regimes.

All the secondary data obtained for this study were analyzed thematically, which involved the extraction of key themes from the respondent's interview transcripts as well as secondary sources.

To conform with ethical standards, the respondents are anonymized while the secondary data were cited and referenced.

Findings

The Computer Emergency Response Team (CERT) acknowledges that addressing cyber security threats requires collaboration from all internet users and actors. This is informed by the fact that whereas governments have the primary mandate of controlling and mitigating national security risks including cyber threats, they usually do not have the direct authority and rights to control privately owned critical infrastructure and assets hence the urgent need for private involvement.

According to the CERT, the major goals of public-private partnerships in cybersecurity include information sharing between public and private entities as well as supporting national cybersecurity strategies, laws, and policies to ensure cyberspace safety. Subsequently, public-private partnerships also present diverse benefits to private organizations. This can be evidenced form the findings; "Collaboration between the private sector and the public sector on cyber security grants the private organizations an opportunity to be actively involved in crafting solutions and strategies aimed at addressing cyber security threats. In fact, the collaboration warrants the private sector more opportunities to gain additional knowledge on how to mitigate vulnerabilities and threats to cybersecurity".

Furthermore, some of the private sector representatives have held the view that cyber security regulations, which would be products of public-private partnerships are most likely to impose substantial costs that may reduce the profitability of the private sector. A private business will have to incur high costs in installing information infrastructures which are critical for cyber safety. Moreover, the private sector also assumes that partnership with other stakeholders including government agencies on cyber security would result in increased information sharing which may lead to the confidentiality and privacy of private business entities' data and information being compromised.

Despite this growing reluctance of the private sector to partner effectively with government agencies, governments have instituted policies, strategies and laws that provide mandatory requirements that private entities must comply with to preserve that state's cyber security. This is because public-private partnership in cyber security is considered very critical for purposes of facilitating communication between the public sector and the private sector and also supporting national cyber security strategies.

Information Sharing as a Role in Public - Private Partnerships

Respondents acknowledged that one of the critical mandates of the private sector as far as cyber security is concerned is information sharing. Carr, (2016), the provision of actionable and timely cyber threat and alert information is a major expectation of the partnership between the private sector and public sector in cyber security. This implies that the private sectors have a role to communicate to the government and other cybersecurity stakeholders about their system vulnerabilities so that efficient actions can be undertaken by relevant parties. In this study, it was noted that in order for mutual collaboration between the private sector and the public sector in communication to exist, both parties must develop mutual trust among themselves. Subsequently, there is a need for the government and the private sector to mutually agree on the communication methods to be integrated, channels, rules of communication, and the specific agencies or entities that shall store the information and how the sensitive information shall be utilized.

This was informed by the fact that the private sector is less likely to share critical cyber security information with the public or government if there was no well-established trust among the parties. The private sector expects that upon sharing with the government critical information on their cyberspace, especially on their system vulnerabilities, no breach of their confidentiality and integrity rights would be violated, (Christensen, & Petersen, 2017).

According to Carr, (2016), there exist several barriers that limit the private sector's ability and willingness to perform their role of willingly sharing critical information with the government on cyber security. Firstly, the respondents noted that in most instances, it is not easy to immediately establish the nature of a cyber-attack and whether or not it is sustainable at the organizational level or whether it is a large-scale sustainable attack that needs expert intervention from the government agencies. This was noted in the study as the private sector is usually reluctant to share cyber security information and even cyber security best practices for fear that if it shares information with the government or other concerned parties about an attack, the information may be leaked to its competitors and this may jeopardize its operations.

According to the findings of the study, it was highlighted that the public sector should also share critical cyber-related information with the private sector. The public sector is obliged to share relevant information on unforeseeable vulnerabilities or cyber risks with the private sector so that the private sector can put in place action plans to address such gaps. Subsequently, the public sector can share with the private sector best practices that if implemented can result in the protection of the private sector cyberspace. This came out from the study as; private sector companies can share critical cyber threats and intelligence cyber information with the public sector and vice versa. This is very crucial for purposes of in-depth understanding of cyber-related threats and the development of efficient and effective strategies to mitigate the risks. Subsequently, when the public sector conducts audits and assessments periodically on their systems and those of the private sector, they should willingly share the results of the assessments with relevant agencies so that best practices of cyber security can be developed.

Noteworthy, the public sector has also remained reluctant to share very critical cyber security information with the private sector due to the sensitivity of such information. The government has remained reluctant to share sensitive information with the private sector. Therefore, the lack of trust and goodwill by both the private sector and the public sector continues to frustrate efforts to establish a synergy of communication between the private sector and the public sector on cyber security.

Innovation as Role in Public- Private Partnerships

Public-private sector partnership remains very critical in cyber security because the collaboration between the private sector, public sector and other agencies. This presents better opportunities for the private sector to offer innovation, agility and specialized knowledge in addressing cyber security threats, (Cavelty & Egloff, 2019). The private sector remains a very critical force for the technological development of cyber security systems. They have continued to play key roles in developing and even investing in key technologies including robotics, artificial intelligence and quantum computing among others.

Therefore, through public-private partnerships, both the private and the public sector enjoy the leverage to share their expert opinions and knowledge on the dynamics of cyber threats which may be very critical for developing new approaches and mechanisms of addressing cyber threats, (Cavelty & Egloff, 2019). This was well captured by the study findings; “ the private sector has the resources and expertise to develop innovative cyber-related solutions that can be relied upon to mitigate the risks of online cyber-related attacks as well as other forms of cyber-crime. Collaborative research between the public sector and the private sector and other agencies can therefore aid in accelerating the pace of innovation and bringing new approaches and ideas in managing cyber threats".

Also, the study acknowledged that the innovative role of the private sector in cyber security has remained constrained by a variety of factors. Firstly, most private organizations lack adequate resources and personnel to conduct adequate research that can result in the generation of new ideas and knowledge in the war against cybercrime. Innovation requires lots of commitment to time, resources, and personnel, which some of the private entities may not be able to sustain. Subsequently, the private sector has been reluctant to share their innovative ideas with the public sector and other agencies, due to a lack of trust in the private sector especially in maintaining their copyrights, using the innovative ideas responsibly including respect for the confidentiality and privacy of the private sector.

5.3 Public-Private Partnership as a Tool for Cyber Awareness and Education

Cyber awareness and sensitization stand out as the key issues in enhancing cyberspace. This is because a clear understanding of cyber risks and threats enables individuals to identify cyber vulnerabilities detect risks and thereafter institute necessary strategies to prevent the occurrence of such risks. The study found out that cyber awareness by both employees and the general public reduces the risk of cyber-attacks by limiting the occurrence of data breaches, phishing attempts, and malware infections among others. This was informed by the fact that cyber sensitization provides the stakeholders with adequate skills and knowledge on how they can protect and secure their data, in the contemporary society characterized by cyber-attacks. The sensitization programs also widen the understanding of stakeholders on cyber regulations and laws, hence the likelihood of mitigating cyber threats and risks.

The private sector has the critical mandate of provision of leadership in educating and sensitizing technology stakeholders including the general public and government agencies on cyber security. They could achieve this mandate by partnering with the government to organize training programs aimed at widening understanding of cyber vulnerabilities, risks, threats, and best practices of cyber security. The private sector and the public sector through the Ministry of Information, Communication and Digital Economy. There is also need to collaborate with multiple stakeholders to discuss cyber threat management in the evolving landscape.

Some of the most important stakeholders in cyber security include technology companies such as Huawei Technologies, Microsoft, Oracle Technologies, Safaricom, Cisco System and Oracle among others. These training programs are equally important because they can also generate innovative ideas to counter the threat of cybercrime. This is well highlighted by the study's finding that the private sector has a mandate to support the government in closing the cyber security skill gap by providing expertise and training to government entities through the provision of critical expertise and also sharing their research findings on cyber security. The awareness and education programs will strengthen the competence level of individuals on cyber security, hence resulting in the adoption of cyber security best practices. Ideally, training programs help organizations improve their situational awareness and make very effective and efficient decisions on their data and systems.

Both the private and the public sectors can offer joint training aimed at bolstering the capacity of the stakeholders on cyber security. The joint training manuals should focus on cyber threat detection, response mechanisms, and strategies to reduce cyber-related vulnerabilities. This is key to the development of cyber defense postures. Joint training on cyber security is ideal as it fosters sharing resources for supporting cyber-related sensitization and education programs. The private sector collaborations in the form of joint training should also focus on highlighting the roles and responsibilities of every stakeholder in cybersecurity and an enhanced understanding of the major regulations and laws that guide cybersecurity.

Some of the challenges that limit private entities' abilities to perform their roles of training and sensitization of the general public on cybersecurity. This assertion is backed by the study's finding which states that,"public awareness and sensitization on cyber security demands commitments to personnel, time, infrastructure and even money, which may be out of reach by most of the private businesses. Subsequently, the private sector may also lack comprehensive training manuals or curriculum to complement their training programs.

In an attempt to address these limitations, private partnerships and collaborations with government agencies result in the development of joint training, which implies shared costs of the training and sensitization. Through partnerships, the public and private sectors may use mass media platforms and social media platforms to sensitize the public on best practices of cyber security.

Collaboration in Developing Norms and Regulations Guiding Cybersecurity

The private and public sectors stand out as the key actors in cyberspace. This is because of the stake they have in the cybespace. Both the private and public sectors therefore have a collective mandate to actively involve themselves in the processes of crafting solutions and mechanisms that concern addressing or mitigating cyber threats, (Juma, Arman & Hidayat, 2023). The private sector and the public sector should therefore provide input and suggestions on the processes of developing national cybersecurity strategies. This is backed up by the study's finding that, "both the private and the public sector should collaborate on cyber security policies and regulations development to facilitate the development of very effective cybersecurity measures that align well with existing legal frameworks".

Ideally, the private sector should actively support the implementation of Kenya's National Cybersecurity Strategy, (NC4, 2022). This will be achieved by not only implementing its provisions but also providing necessary feedback that can aid in ensuring that the strategy aligns well with contemporary cyber security dynamics. The private sector is expected to write policy briefs and proposals that present alternative approaches to addressing the growing cyber security risks in the country. For instance, the media as a private sector entity can support the development and implementation of cyber security policies and frameworks including Kenya's Data Protection Act by providing a viable platform for sensitizing and educating the general public on their cyberrights and best practices to ensure they don't fall victims of cyber-attacks. Furthermore, the media isentitled to share policy briefs and proposals to develop cybersecurity strategies and legislation.

Noteworthy, public-private partnerships are also critical for purposes of standardization of policies and processes that guide cyber security. This is informed by the fact that collaboration of all the key actors of cyber security fosters harmonization of cyber security goals, objectives, interests, and sharing of experiences. This results in the formulation of cyber security best practices, (Juma, Arman & Hidayat, 2023). This is achievable given that the private sector is usually constituted of technical expertise whose inputs can be critical to the development of very effective and efficient cybersecurity frameworks.

The private sector in partnership with other stakeholders can periodically conduct system audits to confirm the suitability and efficiency of existing cyber security procedures and strategies and suggest areas that need improvement to deter system attacks. This is in consistent with the study's which states that when it comes to cyber security, the goal is not only compliance with laws and regulations but also guarding business, individuals and government actors against the dangers of persistent cyber-attacks or threats. The private sector can assist the government in developing counter-cyber security strategies by offering their expert opinions and suggestions during policy reviews and even formulation processes. They can also support counter-cyber security frameworks by being policy advocates, involving sponsoring, organizing and funding cyber security sensitization programs.

The private sector is not only subject to internal cyber security regulations but also to national regulations on cyber security. In an attempt to limit, cyber-related vulnerabilities, there is need for both the private and public sectors to enhance compliance with existing laws to guard their systems from cyber-attacks. This should involve strengthening cyber infrastructures which encompasses integrating information systems with firewalls, passwords and other security measures. For instance, both the private sector and public sectors were obliged to adhere to the provisions of the Computer Misuse and Cyber Crime Act No. 5 of 2018. The act is supported by the Data Protection Act No. 24 of 2019 which provides the necessary guidelines that must be adhered to by all the stakeholders including the private sector for data management, so that important information of organizations do not get into the hands of third parties.

Resource Mobilization

Integrating necessary critical infrastructure for detecting and preventing cyber-attacks demands lots of resources that the public sector and other agencies may not possess. The private sector being a profit-making entity is obliged to be a force in the process of mobilizing resources aimed at facilitating cyber security programs including sensitization, and adoption of modern technologies that detect and deter the occurrence of cyber-attacks. The private sector therefore can play the financial and personnel gap, that exists in developing sustainable systems that deter cyber-attacks. As one of the study's findings points out, "cyber threat deterrence is a shared responsibility. The private sector is expected to be at the forefront of supporting research programs and other programs that focus on establishing a cyber-friendly environment. With closer partnership and collaboration with the public sector, both sectors can gain grants aimed at supporting their initiatives in cyber security. Therefore, the public-private partnership is a strategic approach towards pooling of resources".

Public-private sector partnership is critical for purposes of sharing threat intelligence for purposes of neutralizing cyber threats. For instance, a responsible private sector is expected to share anonymous cyber behaviors with other parties including the public sector for proper cyber action. This can be seen in one of the study's findings, "To combat cyber threats, cyber security actors must combine efforts because cyber threats involve shared risks. The collaboration and partnership are critical for developing in-depth knowledge and understanding of the threat landscape including cyber trends and their evolving nature. Subsequently, the private partnership is also supportive of establishing a stronger and coordinated workforce that is focused on fighting cyber-attacks. In fact, partnerships are significant for sharing experiences on cyber threats and this may be central in the development of cyber policies, strategies, and laws".

Conclusion

The study established that trust and information sharing issues, disclosure and exposure risks, differences in cyber security laws and policies and privacy rights are among the main issues that hinder public-private partnerships. It also found out that public-private partnerships are very critical because they help ing mitigating cyber security issues and fill in the gaps that hinder the war on cyber security. The study highlighted that public-private partnerships foster information or data sharing on cyber security and innovations. This facilitates the development of effective regulatory frameworks that guide cyber security. Subsequently, public-private partnership is a key strategy to fill in the resource gaps on cyber security given that it enables resource sharing between the public and the private sector in so far as mitigating cyber threats is concerned. Therefore, the partnership is very critical for resource mobilization. The study also established that public-private partnership is a key incentive for cyber security sensitization and education, a key step towards minimizing cyber vulnerabilities. Thus the study concludes by reiterating that addressing cyber security threats is a shared responsibility of all actors of cyber security. The actors drawn from both the private and the public sectors should develop common visions, missions, strategies, frameworks, processes and procedures for mitigating cyber security threats.

Recommendations

- **Development of effective and efficient systems of data sharing**

  The private and public actors should promptly share information and intelligence on cyber threats to the public sector and vice versa. This will enhance effective cyber security actions can be undertaken and defensive strategies adopted to prevent the occurrence of similar cyber security risks.

- **Developing effective cyber security inter-agencies**

  The agency should have its membership drawn from both the private and public sectors. The body should be mandated and tasked to develop a synergized operation between the private and the public sectors

- **Conducting Periodic Joint Audits and Assessments**

  Audits and assessments are critical to detecting cyber threats and vulnerabilities. This informs the development of defensive strategies and mechanisms that will be relied upon to prevent cyber-attacks in future. The audits and assessments can be jointly conducted and should involve all the stakeholders of cyber security including but not limited to public sector and private sectors. These audits and assessments should be conducted bi-annually. Organizations should also develop internal mechanisms for conducting audits and assessments frequently.

- **Joint pooling of resources**

  Cyber security is a shared responsibility. Public-private partnerships provide the best platforms for accessing more resources, personnel and experiences that are very critical for running cyber security programs and agendas and countering cyber security threats and vulnerabilities.

- **Critical Infrastructure Protection**

  Organizations must develop internal mechanisms for monitoring and evaluation of cyber systems to ensure that the systems are protected against any form of cyber attack or compromise.

- **Joint Training and Sensitization on Cyber Security**

  The Private sector needs to lead in efforts to mitigate cyber threats by organizing training and sensitization programs. These activities should target all the users of technology. During the training, the participants should be taught some of the risk factors of cyber-attacks and prevention strategies that individuals and organizations can put in place to prevent any form of cyber-attack.

- **Strengthening Frameworks and Laws on Cyber Security**
  There is a need to enhance the implementation and compliance of cyber security laws and regulations including the Cybers Security Acts among others.
- **Establishing a joint effective Incident Response and Emergency Management Unit**
  This unit will be of importance especially in coordinating cyber security incident responses and designing emergency management plans.
- **Further Reasearch**
  The resaerchers, scholars and academicians should conduct further research so as to find out other roles other than the ones which have been mentioned in this study. This is so as the body of knowledge requires to have more information and knowledge concerning this particular field.

References

CAK, (2017). Communications Authority of Kenya, 2017.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43-62.

Cavelty, M. D. and Egloff, F. J. (2019). The politics of cybersecurity: Balancing different roles of the state. *St Antony's International Review*, *15*(1), 37-57.

Christensen, K. K. and Petersen, K. L. (2017). Public-private partnerships on cyber security: a practice of loyalty. *International Affairs*, *93*(6), 1435-1452.

Etzioni, A. (2014). The Private Sector: A Reluctant Partner in Cybersecurity. *Georgetown Journal of International Affairs*, 69-78. https://www.jstor.org/stable/43773650

Juma, A. H., Arman, A. A., & Hidayat, F. (2023, September). Cybersecurity Assessment Framework: A Systematic Review. In *2023 10th International Conference on ICT for Smart Society (ICISS)* (pp. 1-6). IEEE.

NC4, (2022). National Cybersecurity Strategy 2022-2027, 2022.

O'Halloran, J. (2017). *Challenges of Public-Private Partnerships in Cybersecurity* (Doctoral dissertation, Utica College).

Rao Jangili Srinivasa and Thatikonda Anvesh, (2023). "The Role of Cyber Forensics in Addressing Cyber security Challenges in Smart Cities" *Journal of Science and Technology*, Vol. 08, Issue 10, Oct 2023, 1-10.

Tropina, T. and Callanan, C. (2015). Public-private collaboration: Cybercrime, cybersecurity, and national security. *Self-and co-regulation in Cybercrime, cybersecurity and national security*, 1-41.

US, (2017). Statement for The Record Worldwide Threat Assessment of The US Intelligence Community; May 23, 2017.

Van Goethem, E. and Easton, M. (2021). Public-Private Partnerships for Information Sharing in the Security Sector: What's in It for Me? *Information & Security*, *48*, 1-15.