Implementing the Cyber Security Act in Public Financial Institutions in Ghana

What are the Constraints and Enabling factors?

Emmanuel Awuni Kolog
Operations and MIS, University of Ghana
Accra, Ghana
Email: eakolog@ug.edu.gh

Tijani Mohammed
Operations and MIS, University of Ghana
Accra, Ghana
Email: mtijani003@st.ug.edu.gh

Abstract— **The Cyber Security Act of Ghana was enacted as a result of the National Cyber Security Policy and Strategy in Ghana. However, two years after its implementation, progress has been slow. This paper aimed to explore the constraints and enabling factors affecting the implementation of the Cyber Security Act in Ghana, based on the International Communication Union's pillars of cybersecurity. A mixed-method approach was used, with data collected from 168 respondents through a questionnaire and interviews. The survey data was analysed using Partial Least Square- Structural Equation Modeling (PLS-SEM), while the interview data was analysed using theory-based content analysis. The study found that financial institutions in Ghana have satisfactory policies and regulatory measures on cybersecurity, but lack the technical capacity to implement them effectively. The study also revealed satisfactory organizational and capacity development measures, but more awareness creation and organizational support are needed, including budget allocation and support from top management, to effectively implement cybersecurity policies in Ghana.**

Keywords- information security; cyber security act; public financial institutions; Ghana.

I. INTRODUCTION

Governments and organizations worldwide are increasingly utilizing Information and Communication Technologies (ICTs) to promote economic growth and national development [1]. However, the growing number of Internet users globally is hindering this progress. As of April 2022, there were over 5 billion active Internet users and approximately 1.92 billion websites, making cyber monitoring and control extremely difficult [2]. This development has also made cyberspace more susceptible to attacks and exploitation. Cybersecurity breaches can be catastrophic, resulting in loss of life, financial loss, and business collapse. Infamous cyberattacks, such as those on Sony Pictures, the USA pipeline shutdowns, and the NotPetya virus, for instance, were reported to have caused over US $10 billion in damages [3].

On December 29, 2020, Ghana's President assented to the 2020 Cyber Security Act 1038 [7]. The policy's aim is to provide a secure cyberspace to support the country's digitalization agenda and its transition to a knowledge-based economy. The Act draws on eight frameworks from Ghana's National Cybersecurity Policy and Strategy (NCSPS): legislative and regulatory frameworks, cybersecurity technology frameworks, culture of security and capacity building, research and development towards self-reliance, compliance and enforcement, child online protection, cybersecurity emergency readiness, and international cooperation frameworks [8].

The Act contains 100 sections and three schedules and assigns it to a Cybersecurity Authority (CSA) [8]. The CSA's objectives include regulating, managing, and promoting cybersecurity issues, as well as preventing and responding to cyber threats and incidents in Ghana. Sections 5 to 34 outline the CSA's structure, administrative provisions, financial provisions, and the establishment of a cybersecurity fund to support the authority's operations. Sections 41 to 48 provide for the establishment of national and sectoral computer emergency response teams (CERT) and cyber security incident reporting (CIRT). Licensing of cybersecurity service providers, accreditation of cyber professionals, and certification of cyber products are covered in Sections 49 to 58. The Act also promotes cybersecurity standards and their enforcement, public awareness and education as detailed in Sections 59 to 61.

As ICTs continue to fuel economic growth and national development, the number of active Internetusers worldwide has surpassed 5 billion, with over 1.92 billion websites as of April 2022 [2]. However, this increased digitalization has also made cyberspace vulnerable to cyber attacks, which can have severe consequences such as loss of life, financial loss, and business collapse. To address this, countries and organizations worldwide are now incorporating cybersecurity regulatory measures into their national and sectoral security strategies. In Ghana, the government is pursuing an ambitious digitalization agenda, which has led to increased cyber-related activities among government agencies, private sector institutions, and citizens. However, this has also led to an increase in cybercrime and cyber threats [5], such as ransomware, identity fraud, blackmail, online child exploitation, and social engineering.

This study aims to explore the implementation of Ghana's Cybersecurity Act 2020 (Act 1038) by public financial institutions and investigate the constraints and enabling factors needed to improve its implementation. The study is divided into six sections. Section I introduces the study and emphasizes the importance of the topic. Section II presents the study's framework and the development of its hypotheses. In Section III, the methodology is discussed, including data collection and analysis methods. Section IV presents the study's findings, while Section V interprets and discusses the results in depth. Finally, in Section VI, the paper concludes by summarizing the main points and drawing conclusions about the implementation of the Cybersecurity Act.

II. FRAMEWORK AND HYPOTHESIS DEVELOPMENT

In the section, we present the study’s conceptual framework and **the** hypothesis development.

A. *Framework*

A comparative analysis of current international cybersecurity indexes by [10] [13] identified three key frameworks developed by cybersecurity experts and globally accepted for evaluating cybersecurity capacities: the Global Cybersecurity Index (GCI) by the ITU, the National Cybersecurity Index (NCSI) developed by the e-Governance Academy Foundation, and the Index of Cybersecurity (ICS) developed by the New York University Centre for Cybersecurity. Table I presents the GCI framework, which shows the various constructs.

TABLE I. MAPPING ITU MEASURES TO GHANA'S NCSPS

ITU Measures	Corresponding NCSPS Framework
Legal	▪ Policies and regulatory framework ▪ Compliance and enforcement measures ▪ Child online protection
Technical	▪ Cyber security technology framework ▪ Cyber security emergency
Organisational Capacity Development	▪ Effective governance ▪ Culture of security and capacity building ▪ Research and development towards self-reliance
Cooperation	▪ International cooperation

Although each framework seeks to measure cybersecurity capacities at the national and organizational level, their application and context vary because they have different systems of indicators and evaluation. The GCI is the most comprehensive and widely accepted framework, and it is used in this study.

B. *Hypothesis Development*

The legal measures, as presented in Table I, focus on the presence of legal and regulatory frameworks, which serve as the foundation of all cybersecurity policies. These measures provide clear guidance for cybersecurity governance and include indicators such as regulations for prosecuting cybercrime, protecting online identities and data, child online protection, privacy, system breaches, cybersecurity audits, implementation of standards, and identification and protection of Critical Information Infrastructure (CII) [10]. The implementation of these measures provides legal support in the form of policies and procedures that protect individuals and CII from exploitation and harm [11]. The question now is whether financial institutions are adapting to Ghana's 2020 Cyber Security Act 1038 or revising their existing policies to align with it. This leads to the first hypothesis of this study:

H1: Financial institutions in Ghana have legal measures to implement cyber security Act

The technical measures focus on the presence of structures and mechanisms to address cyber threats and incidents. This pillar acknowledges the significance of national and sectoral Computer Incident Response Teams (CIRT) and Computer Emergency Response Teams (CERTs) in promoting cyber resilience. Technical capacity also includes the existence of standards and baseline requirements for the deployment and use of technological resources. As technology is rapidly advancing, the technical capacity and technologies necessary to combat cybercrime and enhance national cybersecurity must also be continually improved to remain relevant. The 2020 Cyber Security Act 1038 contains provisions for establishing national and sectoral CERTs, CIRTs, and early warning systems, developing system standards, and capacity building [10]. Therefore, the study hypothesis is:

H2: *Financial institutions in Ghana have the technical capacity to implement cyber security Act*

The organizational measure examines the IT governance structures, including the establishment of cybersecurity objectives and strategic plans, as well as the formal definition of institutional roles and responsibilities to ensure accountability [10]. It assesses the existence of a central governing body and how it coordinates with various departments to implement and enforce these regulations. Key organizational indicators include the existence of a legitimate and enforcement authority; organizational cybersecurity strategies with an action plan; protection of Critical Information Infrastructure (CII); and a clear definition of roles and accountability for key stakeholders. Therefore, the third hypothesis for this study is:

H3: *Financial institutions in Ghana have organizational capacity to implement cyber security Act*

The *Capacity measure* involves activities required to increase human and institutional knowledge [10]. This measure supports the development of cybersecurity solutions to prevent and respond to threats and cyber risks. Under resource constraints environment, risk of cyber threats is higher because of absent or limited tools and technical knowledge [17]. Capacity building includes targeted awareness campaigns; a system for certification and accreditation of cyber security professionals and service providers; support for professional training packages in cybersecurity for key stakeholders; and the inclusion of cybersecurity in training programs. Other capacity-building measures also include research and development; the existence of a cybersecurity industry to support the development of cyber security products and services; and the growth of cyber start-ups. The study thus, hypothesize that:

H4: *Financial institutions in Ghana have developed a capacity building measures towards awareness of the Act.*

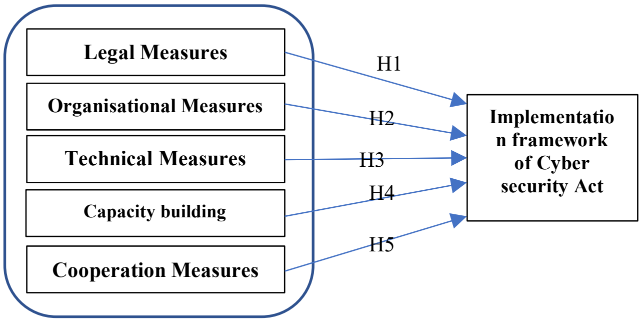

Figure 1. Conceptual framework

Cybercrimes are borderless and transnational; hence, promoting cybersecurity requires *collaboration and* *cooperation amongst* internal stakeholders and external agencies [17]. This requires a multi-stakeholder approach, including bilateral and multilateral agreements; participation of industry forums, international fora/associations; public-private partnerships; inter-agency partnerships; and alluring to best practices. This also assesses the number of partnerships, cooperative frameworks, and information-sharing networks established to build capacity and cyber resilience. Hence, we hypotheses that:

H5: *Financial institutions in Ghana are collaborating and cooperating to implement Act*

III. Methodology

The purpose of this section is to provide an overview of the approach and methodology used in the study

A. Research Approach and Data collection

A mixed research method was chosen for this study in line with its purpose. An empirical review was conducted to identify the constraints and enabling factors in the implementation of cyber security policies. The review revealed that a quantitative method combined with a qualitative approach would be the most appropriate way to gather data and insights from subject matter experts in the field of cybersecurity [13].

To achieve this, a survey questionnaire was developed along with structured interview questions for qualitative insights [14]. Efforts were made to ensure that the questionnaires relating to the hypothesis and conceptual framework could accurately ascertain discriminant validity and reliability [15]. The questionnaires used in this study were adapted from ITU's model questionnaires for cyber security evaluation (see Table II). Data was collected using online survey questionnaires and semi-structured interviews conducted simultaneously.

TABLE II. Mapping ITU Measures to Ghana's NCSPS

	Constructs	# of Items	Source
1	Legal measures	LM (7)	ITU-GCI, NCSSP
2	Technical measures	TM (7)	ITU-GCI, NCSSP
3	Organisational measure	OM (7)	ITU-GCI, NCSSP
4	Capacity measures	CD (5)	ITU-GCI, NCSSP
5	Cooperation measures	CM (4)	ITU-GCI, NCSSP

A purposive sampling technique was used, and survey links were sent to about 200 staff of financial institutions in Ghana. This provided a wide population reach to supplement the interviews conducted with 14 IT managers and chief information security officers (CISOs) from selected financial institutions.

B. Method of Data Analysis

A total of 154 valid responses were received from the survey, and data cleaning was performed. The data from the Likert scale were coded into numerical values for easy analysis. For close-ended responses, partial least squares structural equation modelling (PLS-SEM) was used for analysis. PLS-SEM is recommended for quantitative data analysis as it provides tools for estimating multiple and interrelated dependencies in a single analysis, which tends to provide a high level of predictive accuracy [16]. SmartPLS software was used as it is more feasible for measuring and developing comprehensive structural and predictive models.

IV. Results

The study's result is presented in this section.

A. Demorgraphic

Respondents spanned 12 banks and 4 rural banks in Ghana, with an average of 10 staff from each institution. 52 of the participants were females (34%) with the remaining being male (66%). For age distribution, there were distinct age groupings, which were Gen X, Gen Y, and Gen Z. Interestingly, the lowest level of education of the participants was bachelor's degree holders. Table III shows the summary statistic of the demographic data.

TABLE III. Participant Demography

Category	Variable	Frequency (N=154)	Percentage
Gender	Male	102	66
	Female	52	34
Age	18-23 years	6	4
	24-39 years	128	83
	40-55 years	20	13
Education	Bachelor	78	51
	Masters	76	49
Employment Level	Operational	90	58
	Middle mgt	52	34
	Top Mgt.	12	8

We assessed the respondent's knowledge of the Cyber Security Act in Ghana. From the results in Table III, 69% of participants were aware of the Act, with 31% not being aware. A question on cyber security attributes was asked by providing six options as follows: confidentiality, security, availability, protection, reliability, and policies. The respondents were tasked to select those that they know.

B. Cyber Act Implementation in Ghana

In using PLS-SEM to analyse the quantitative data, a 3-stage approach involving initial estimates of the measurement model and the structural model was developed, after which a final estimate for both the measurement and structural model was constructed.

1) Measurement Model Assessment

The latent variable with the indicators is reflective, hence, in its assessment, an analysis was conducted on the size and significance of the loadings, construct reliability, and convergent and discriminant validity [17]. The purpose of these assessment was to test for the relationship between indicators and constructs to ascertain their relevance. The initial step in measurement model assessment was to assess the indicator loadings of each construct. According to Hair *et al.* [12] loadings at 0.70 and above indicates that the construct explains more than 50% of the indicator's variance. As indicated in Table IV, some of the indicators were weak and deleted eventually.

An assessment of the reliability of the constructs was undertaken to identify the degree to which the indicators measuring the same constructs are related. This was done using Cronbach's alpha and composite reliability. However, for reflective PLS-SEM models, composite reliability is preferred to Cronbach's alpha because Cronbach's alpha can over or underestimate reliability due to its usage of the entire model for estimation [18]. Higher values indicate higher levels of reliability when interpreting construct reliability with a value at 0.70 and above preferred [16]. The composite reliabilities of the constructs in the research model are all above 0.70, indicating reliability among constructs to their indicators as shown in Table V.

After satisfying indicator and construct reliability, construct validity was performed to measure the extent to which the defined construct in the research model measures what it is intended to measure, such as legal measures truly measuring only legally related indicators. This assessment was done using convergent and discriminant validity.

TABLE IV. CONSTRUCT LOADINGS

	CD	CM	LM	OM	TM
CD2	0.912				
CD3	0.923				
CM1		0.870			
CM2		0.812			
CM4		0.902			
LM1			0.927		
LM2			0.906		
LM7			0.779		
OM1				0.969	
OM2				0.967	
TM1					0.903
TM2					0.912
TM3					0.919
TM5					0.903
TM7					0.932

Convergent validity examines if two interrelated constructs in the model are theoretically connected. This is also referred to as communality and it is measured with Average Variance Extracted (AVE). AVE value above 0.50 is always desired [20]. From Table V, all the constructs' AVE exceeds 0.50 which is above the desired threshold.

TABLE V. CONSTRUCT RELIABILITY AND VALIDITY

Constructs	Cronbach's Alpha	rho_A	Composite Reliability	AVE
Capacity	1.000	1.000	1.000	1.000
Cooperation	1.000	1.000	1.000	1.000
Implementation framework	1.000	1.000	1.000	1.000
Legal	0.843	0.871	0.905	0.762
Organisational	0.933	0.933	0.968	0.937
Technical	0.953	1.125	0.962	0.835

TABLE VI. HETEROTRAIT-MONOTRAIT RATION MATRIX=

	CD	CM	IF	LM	OM	TM
Capacity						
Cooperation	0.765					
Implementation framework	0.328	0.169				
Legal	0.313	0.216	0.876			
Organisational	0.786	0.590	0.269	0.293		
Technical	0.576	0.429	0.170	0.126	0.699	

Discriminant validity is the last assessment done in the measurement model. This determines that two unrelated constructs are theoretically not connected. Three approaches are generally used to assess discriminant validity. They are Fornell and Larcker's [19] criteria, cross-loadings, and the Heterotrait-Monotrait Ration (HTMT) criterion [9]. However, PLS-SEM recommends using HTMT.

The HTMT criterion estimates the true correlation between two constructs as if they were perfectly reliable. HTMT value above 0.90 suggests a lack of discriminant validity. From Table VI, all constructs in our model score below 0.90, hence the indication of model discriminant validity.

2) Structural Model Assessment

After satisfying all the measurement model requirements, an assessment is conducted on the structure of the model to test the hypothesis of the study. Multicollinearity amongst constructs is assessed using the variance inflation factor (VIF). Higher VIF indicates critical levels of collinearity, with values below 5 being desirable. Table VII shows the VIF values for the constructs in the research model, with the highest being 3.987, indicating good indicator collinearity. Higher VIF indicates critical levels of collinearity, with values below 5 being desirable. Table VII shows the VIF values for the constructs in the research model, with the highest being 3.987, indicating good indicator collinearity.

TABLE VII. VARIANCE INFLATION FACTOR (VIF)

Constructs	**VIF**
Capacity	3.987
Cooperation	2.422
Legal	1.106
Organisational	2.895
Technical	1.758

Once there are no collinearity issues amongst the indicators, the value of R^2 was computed to determine the in-sample predictive power of the model. R^2 values range from 0 to 1, with higher values closer to 1 indicating better predictability of the structural model. R^2 for this model is 0.710, as indicated in Table VIII, which is closer to the substantial preferred value of 0.75 and greater than the moderate value of 0.5. This indicates that the model predicts by a combined percentage of 71% how legal, technical, organisational, capacity development, and cooperation measures predict the policy implementation framework of the 2020 Cyber Security Act 1038 by financial institutions in Ghana.

TABLE VIII. MODEL FIT WITH R^2

	R^2	**Adjusted R^2**
Implementation framework	0.686	0.675

The effect size represents the change in the coefficient of determination when a specified construct is omitted from the model. This is measured with f^2, where values of 0.02, 0.15, and 0.35 represent small, medium, and large effects, respectively. Thus, values of less than 0.02 indicate no effect, whilst values above 0.15 indicate significant effects. From

Table 4.8, legal measures have the largest effect size with values of 1.788. Capacity had 0.043 which is substantive. Cooperation and technical measures had medium effects with 0.025 and 0.015 respectively. Organisational had no effect with a value of 0.011 which is below 0.02.

Hair *et al.* [20] recommend a minimum acceptable sample size for bootstrapping to be 1000 samples. However, for more reliability, a sample size of 10000 was chosen using a two-tailed distribution with a bias-corrected and accelerated (BCa) bootstrap method. This produced t-values and p-values as shown in Table IX.

At the 0.95 significance level, t-values above 1.96 show significance, whilst values below show no significance. In that order, legal measures, cooperation measures, and capacity measures are significant. t-values of 1.649 and 1.112 for technical and organisational measures indicate they have no statistical significance in this research model.

TABLE IX. EFFECT SIZE

Constructs	Effect size (f^2)
Capacity	0.043
Cooperation	0.025
Legal	1.788
Organisational	0.011
Technical	0.015

Hair *et al.* [20] recommends t-values of at least 196 before a hypothesis can be inferred as supported. Therefore, this model supports three of our hypotheses outlined in Section 3. H_2 and H_3 are rejected based on the t-values. H_1, H_4, and H_5 can be considered viable hypotheses and hence accepted.

TABLE X. CONSTRUCTS SIGNIFICANCE

	Original Sample (O)	Sample Mean (M)	Standard Deviation	T Statistics (|O/STDEV|)	p-values		
Legal =>implementation	0.358	0.356	0.024	15.037	0.000	H_1	**Supported**
Technical -> implementation	0.042	0.042	0.025	1.649	**0.099**	H_2	Not Supported
Organisational -> implementation	-0.045	-0.043	0.04	1.112	**0.266**	H_3	Not Supported
Capacity -> implementation	0.105	0.105	0.045	2.339	0.019	H_4	**Supported**
Cooperation -> implementation	-0.063	-0.063	0.029	2.154	0.031	H_5	**Supported**

C. Constraints and Enabling factors

All the interviewed participants affirmed their knowledge of the 2020 Cyber Security Act and indicated that their organizations are taking steps to implement it. With regards to the frequency of review of cyber security policies, about 90% of the participants suggested 2 years and must be guided by the frequent changes in the threat landscape in the cyber ecosystem. At the organizational level, it is recommended that policies are reviewed annually, but when new threats or technologies emerge, changes in national or international regulations occur, or internal incidents happen that were not captured in existing policies, they should be reviewed and updated. Tables XI and XII are sample extracts (response) from participants during the interview.

TABLE XI. CONSTRAINTS OF IMPLEMENTING CYBER SCEIRTY ACT IN GHANA

	Sample Extract	Identified Themes
1	*"For the implementation, it's fully done. But it's one thing to implement and another to enforce. Now the question is, are we enforcing all the policies in the act as stated??"*	Policy enforcement
2	*"In my opinion, the cost and resources are the constraints. Cost can be broken down into infrastructure and human resource costs. Resources will be human and tools to be used."*	Financial cost, Limited technical capacity, Human resources
3	*"Lack of awareness on the 2020 Cyber Security Act 1038"*	Lack of awareness
4	*"The understanding of Act 1038 is still not too much by the public and the institutions tasked to implement, simply because the institutions tasked to do so may not be doing its job"*	Lack of understanding of the Act, Ineffective organisations

TABLE XII. ENABLING FACTORS FOR IMPLEMENTATION OF CYBER SECURITY ACT IN GHANA

	Sample Extract	Identified Themes
1	*"The first task is to identify those charged to implement it and those charged to ensure more education. Identification of what has been done so far by these two separate bodies will inform the awareness mechanism to undertake. When people get informed, it empowers them to take proactive and preventive actions"*	Collaboration Awareness
2	*"Training of persons in IT roles to enable them to focus on cyber security issues. Government to give waivers for certain cyber security tools or operations for cyber security service providers"*	Training Government support
3	*"Creation of awareness on the Cyber Security Act amongst stakeholders. Capacity building and knowledge transfer between personnel of stakeholder agencies.*	Collaboration, Awareness creation, Capacity building
4	*"Establish and adopt cyber security standards for education, skills development, risk management, research and development and practitioners."*	Cyber security standards, Skills development, Research

V. DISCUSSION

The ITU's Global Cyber Security Index assessed Ghana's cyber security score as 89.69% in 2021, a significant increase from 32.6% in 2017 [6]. This achievement was celebrated by the CSA and the Ghana Ministry of Communication, as it placed Ghana in the 3rd position as the most cyber-committed country in Africa after Mauritius and Tanzania. The assessment evaluated five key pillars, including legal, technical, organizational, capacity development, and cooperation measures [10]. However, the public financial institutions in Ghana still need to fully comply with the ITU's cyber security index despite Ghana's progress in the cyber space due to the implementation of the Act.

The findings of this study indicate that the public financial institutions in Ghana have sufficient legal measures to implement the 2020 Cyber Security Act 1038, which is a crucial determinant of the model's reliability. Financial institutions in Ghana have appropriate policy and regulatory measures on data protection, unauthorised use of computer systems, and cyber security audit and risk management. However, policies on enforcing cyber security standards, managing online harassment, and mitigating cyber security risks are either non-existent or inadequate, despite public financial institutions in Ghana implementing several policy measures

The study findings indicate that financial institutions in Ghana lack adequate technical capacity to comply with the Cyber Security Act 1038. This means that these institutions do not have sufficient technical measures to implement the Act. Despite these technical limitations, financial institutions in Ghana employ only certified cyber security professionals and procure and use genuine software systems, as the risks and implications of using pirated or fake software are high. This is due to the strict directive from the Bank of Ghana, which enforces regulations that require all financial institutions in Ghana to only employ certified IT managers and chief information security officers.

The study rejects the third hypothesis, which states that public financial institutions in Ghana are organized to implement the 2020 Cyber Security Act 1038. Critical organizational measures that are lacking include the absence of a dedicated cyber security unit, and cyber security policies that are not readily available and disseminated [18]. Additionally, the management of financial institutions in Ghana must be more committed to supporting the implementation of the Act through financial support and any other means possible at the strategic level. The supervisory division of the Bank of Ghana could help ensure proper organization of financial institutions in terms of cyber security implementation and enforcement.

The study has found that the capacity building development initiative by financial institutions in Ghana is satisfactory. However, more needs to be done to increase their capacity building initiatives through investing in cyber security infrastructure, research, and providing security education, training, and awareness. In addition, the study identified constraints in the implementation of the Cyber Security Act, including lack of awareness and training, lack of top management support, policy enforcement challenges, lack of understanding of the Act, and user non-compliance. The study also highlighted cross-cutting themes, including awareness creation and training, policy enforcement, cyber security technical measures and standards, human resource development, management support, and collaboration, which need to be addressed to enable the successful implementation of the Act. It is crucial to provide these enabling factors for the implementation of the 2020 Cyber Security Act 1038. Moreover, CSA should be supported and equipped to perform its mandates while developing the capacities of various CIIs and stakeholders necessary to ensure the Act's successful implementation

VI. Conclusion

Based on the Global Cyber Security Index and the Ghana National Cyber Security Policy and Strategy, a conceptual framework was developed to explore the state of the implementation of cyber security in Ghana. Five key themes were identified, which underpin all cyber security policies and implementation strategies. These are legal, technical, organizational, capacity development, and cooperation measures. Questionnaires were administered and interviews were conducted to collect data. The study found that financial institutions have instituted several policy measures but lack the capacity to implement them. In future, we intend to expand the study by exploring he various cyber security techniques being adopted by the financial institutions in Ghana.

References

[1] D. Thapa and Ø., Saebø, “Exploring the link between ICT and development in the context of developing countries: A literature review” The Electronic Journal of Information Systems in Developing Countries, vol 64, no. 1, pp. 1-15, 2014.

[2] Statistica, “Internetusers in the world 2022”. [Retrieved: January 2023] https://rb.gy/7h9ots

[3] M. Hepfer and T.C. Powell, “Make Cybersecurity a Strategic Asset”. MIT Sloan Mgt. Review, vol. 63, no. 1, 4pp. 0-45, 2020

[4] V. Lebogang, O. Tabona., and T. Maupong, “Evaluating Cybersecurity Strategies in Africa”. In Cybersecurity Capabilities in Developing Nations and Its Impact on Global Security, pp. 1-19, 2022.

[5] R. Sabillon, V. Cavaller and J. Cano, ”National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Eng. Vo. 5, no.5, p. 67, 2016.

[6] O. Longe, O. Ngwa, F. Wada, V. Mbarika, and L. Kv asny,“Criminal Use of Informationand Communication Technologies in Sub-Saharan Africa: Trends, Concerns andPerspectives”. Journal of Information Technology Impact, vol 9, no. 3, pp.155-165, 2009.

[7] Paliament of Ghana, “Cyber Security Act 2020”. [Retrieved: January 2023] available at https://rb.gy/al3oky

[8] GNCSP. "Ghana National cyber security policy and strategy” [Retrieved: January 2023], available at https://rb.gy/7u9lfj

[9] J.F Hair, J.J Risher, M. Sarstedt, C.M, Ringle “When to use and how to report the results of PLS-SEM”. European business review. Vol. 3, no. 1, pp. 1-24, 2019

[10] ITU (2015), “Global security index”. [Retrieved: January 2023] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[11] M. Kaur, “Cyber Security Challenges in the Latest Technology”. In Proceedings of Third International Conference on Communication, Computing and Electronics Systems, pp. 655-671, 2022.

[12] J.F Hair, G.T.M. Hult, C.M Ringle, M. Sarstedt, “A primer on partial least squares structural equation modeling (PLS-SEM)”.Sage publications, New York, 2021.

[13] J. Mayoh, and A.J. Onwuegbuzie, “Toward a conceptualization of mixed methods phenomenological research”. Journal of mixed methods research, vol. 9 no. 1, pp. 91-107, 2021.

[14] J.L Myers, A.D Well, and R.F Jr, “Research design and statistical analysis” 3rd ed, Routledge, 2013.

[15] E. Dubois and U. Tatar “Data analysis in research: Why data, types of data, data analysis in qualitative and quantitative research. QuestionPro. [Retrieved: January 2023] at https://rb.gy/apfphh

[16] K.K.K Wong, “Mastering Partial Least Squares Structural Equation modelling ” Universe: Bloomington. IN, USA, pp. 1-184, 2019.

[17] Jr., J. F., Hult, G. T., Ringle, C. M., Sarstedt, M., Danks, N. P., and Ray, S, “Partial least squares structural equation modelling (PLS-SEM) using R: A workbook” no. 1, pp. XIV, 197, 2021

[18] Bank of Ghana (2018). Cyber and Information security directives. [Retrieved: January 2023], https://rb.gy/ylvoz

[19] C. Fornell and D.F, larcker, “ Evaluating structural equation models with unobservable variables and measurement error”. Journal of Marketing Research, vol 18, no. 1, pp. 39–50, 1981.

[20] J., Hair, C, Ringle, and m. Sarstedt, M., “PLS-SEM: Indeed a Silver Bullet”, Journal of Marketing Theory and Practice, no. 19, pp. 139-151, 2011.