LEGON CENTRE FOR INTERNATIONAL AFFAIRS AND DIPLOMACY (LECIAD)

UNIVERSITY OF GHANA

CYBER RISK POSTURE OF GHANAIAN TELECOMMUNICATION COMPANIES: A CASE STUDY OF VODAFONE GHANA

BY

NAA ADAWULEDE ANDREWS

(10390977)

THIS DISSERTATION IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON, IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE MA IN INTERNATIONAL AFFAIRS & DIPLOMACY DEGREE

LEGON **JULY 2021**

DECLARATION

I, NAA ADAWULEDE ANDREWS do hereby declare that, this dissertation is the result of an original research conducted by me under the supervision of Dr. Nene-Lomotey Kuditchar, and apart from other works, which have been duly acknowledged, no part of it has been submitted anywhere for any purpose.

NAA ADAWULEDE ANDREWS (CANDIDATE)	DR. NENE-LOMOTEY KUDITCHAR (SUPERVISOR)
06/08/2022 **DATE: ……**	06/08/2022 **DATE: ……**

DEDICATION

This work is first dedicated to God Almighty for the strength, wisdom, grace and discipline He instilled in me to complete this work. I also dedicate this work to my parents for their support throughout my academic life. I also dedicate this work as well, to My Love for his endless support and encouragement throughout my study and writing of this dissertation.

May God richly bless you all.

ACKNOWLEDGEMENTS

After what seemed to be an endless period of despair, I would like to thank the Almighty God for giving me strength to complete this work. Thank you for hearing me when I was down. All praise and glory unto You.

Secondly, I cannot begin to thank My Love, Mr. Henry Olletey, for his endless support and encouragement. His words, pragmatism and positivity helped me move forward when I felt like I could not any longer. I am truly grateful.

I would also like to thank two special classmates: Ms Nina Ohenewaa Kwarteng, and Mr. Ato Enninful for always finding time to encourage despite struggles with their own work.

My gratitude also goes to all organizations and resource persons who irrespective of their busy schedules made it possible to answer all my questions. Your input is invaluable.

Finally, my sincere appreciation goes to my supervisor, Dr. Nene-Lomotey Kuditchar who provided astute advice and suggestions throughout all review sessions. His feedback always pushed me to amplify and evaluate my ideas.

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
ITU	-	International Telecommunications Union
USB	-	Universal Serial Bus
NCA	-	National Communications Authority
MNO	-	Mobile Network Operator
ERM	-	Enterprise Risk Management
DoS	-	Denial-of-Service
DDoS	-	Distributed Denial-of-Service
CoE	-	Council of Europe
AU	-	African Union
MoU	-	Memorandum of Understanding
ECOWAS	-	Economic Community of West African States
CIRT	-	Computer Incident Response Team
CERT	-	Computer Emergency Response Team
CIIP	-	Critical Information Infrastructure Protection
PPP	-	Public-Private Partnerships
ADP	-	Accelerated Development Program
SAT-3	-	South Atlantic Telecommunications cable no.3
WASC	-	West African Submarine Cable
VSAT	-	Very Small Aperture Terminal
ISP	-	Internet Service Provider
PCSRC	-	Postal and Courier Services Regulatory Commission
GMet	-	Ghana Meteorological Agency
AITI-KACE	-	Ghana-India Kofi Annan Centre of Excellence in ICT

NITA	-	National Information Technology Agency
DPC	-	Data Protection Commission
GIFEC	-	Ghana Investment Fund for Electronic Communications
GPCL	-	Ghana Post Company Limited
NCSPS	-	National Cyber Policy and Strategy
CNII	-	Critical National Information Infrastructure
NCSC	-	National Cyber Security Centre
COP	-	Child Online Protection
NCSTWG	-	National Cyber Security Technical Working Group
UAM	-	User Access Management
CISO	-	Chief Information Security Officer
CTO	-	Chief Technology Officer

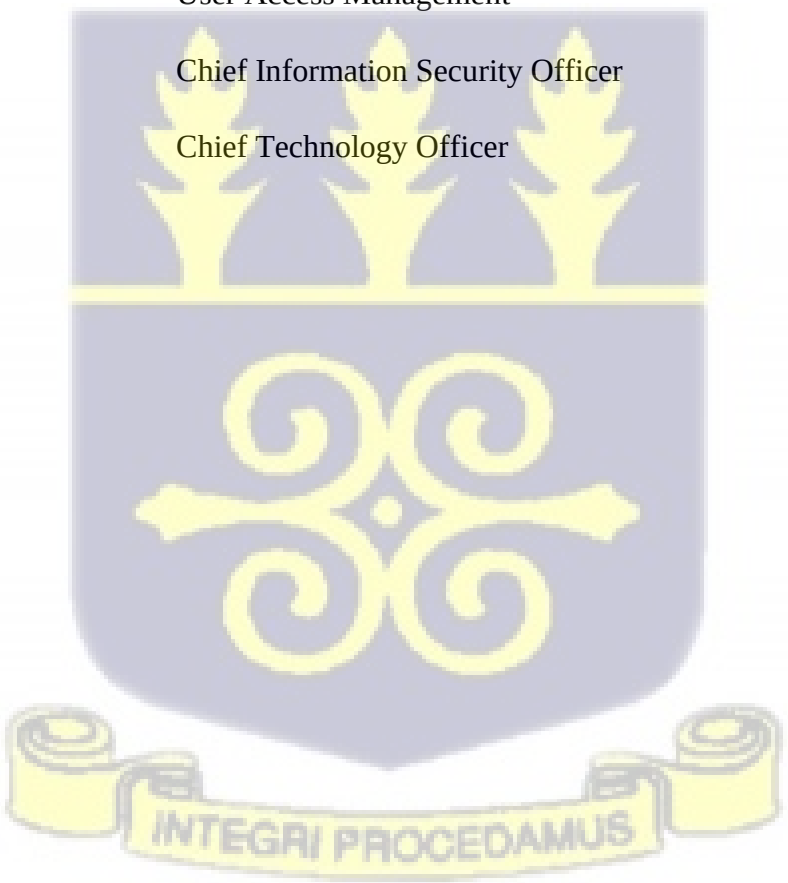

TABLE OF CONTENTS

ABSTRACT

This study sought to explore the cyber risk posture of Ghanaian telecommunication companies using Vodafone Ghana as a case study. This study used Enterprise Risk Management (ERM) as a theoretical backbone and data were collected and analyzed qualitatively. Scholars define ERM as a holistic, systematic, and integrated approach to the management of the total risks that a company faces. It challenges the norm of siloed and department-specific risk management. The risk management structure and approach of the organization largely follow the tenets of ERM and outlined how cyber risks are identified, mitigated and monitored at different levels. The findings further indicated that telecommunication companies in Ghana experience unique cyber risks due to their capacity in storing and handling sensitive information in operations. Also there seems not to be cross-firm collaboration and experience sharing on the application of the ERM strategy. It seems organizations operate in isolation when it comes to the need of protection against cyber risks. In addition, although Ghana's national cyber policy evolution and current state is adequate relative to regional and global standards, the enforcement and enactment of provisions is lax and lacking at best. Recommendations from this study are based on ways to enhance cyber security posture in the telecommunications industry and the country. These include collaboration between industry players, public sector collaboration, regional/international cooperation, and awareness campaigns to develop public culture on cyber security.

CHAPTER 1
Cyber Security and Risk Management

1.0 Introduction

Advances in technology have brought the world to a new age; the fourth industrial revolution or Industry 4.0. This shift heralds a cyber-connected world with increased smart machinery, manufacturing, tailored products and services, smart autonomous technologies, artificial intelligence, Internet of Things (IoT), and cloud computing among others (Deloitte, 2017). As of July 2020, there are 4.57 billion active internet users worldwide (Clement, 2020). The interconnectedness of Industry 4.0-driven operations coupled with the speed of digital transformation proliferates increasingly complex cyber risks and cyber security challenges (Deloitte, 2019). These cyber risks force people, organizations, institutions and governments to alter their manner and culture of operations to achieve strategy and business objectives. Organizations of all types and sizes are susceptible to cyber-attacks with valuable data, systems, and assets at the mercy of cyber attacker's motives. Increasing cyber threat activities prevent organizations from achieving strategy and business objectives and can result in destruction and deterioration of trust, brand, reputation, informational assets and financial well-being of victim companies. As a result, the reality is that cyber risk is not something that can be avoided; instead, it must be managed.

According to International Telecommunications Union's (ITU) global cyber security index conducted in 2018, Ghana ranked 89th out of 175 nations (International Telecommunications Union, 2019). In 2019, Ghana lost about $9.8 million to criminal activities last year, compared to $105 million dollars in the previous year to cybercrime acts including mobile money scams, and other forms of extortion (Nyarko-Yirenkyi, 2020). With the emergence of cyber-fraud crime between 1999 and 2000 in Ghana, the evolution of electronically based crimes has been from credit card fraud, initially facilitated by hotel attendants at international hotel chains who would collate and share credit card details of Western visitors with scammers. There were also

identity or romance scams where fraudsters posed as individuals with false identities faking love interests for financial information and passwords; estate fraud where scammers 'sell' property to typically Westerners and Ghanaians residing in the diaspora looking to return to the country upon retiring; all of which were infamously termed as 'sakawa' or '419 schemes' (Warner, 2011, pp. 739,740,744). The proliferation of cyber-crime drew attention to the country and resulted in being blacklisted as a haven for money-laundering by the transnational surveillance agency, the global Financial Action Task Force in 2012 (Darko, 2015) and flagged by U.S. online retailers as they became increasingly aware of fraudulent orders from internet scammers (Warner, 2011, p. 738).

Ghana was among the first nations on the continent to gain access to the internet in the 1990s (Foster, Goodman, Osiakwan, & Bernstein, 2004, p. 6). Access to internet connectivity was in waves beginning from computers in internet cafés and other public access areas such as workplaces, schools and tertiary institutions. The second wave of internet connectivity was through the introduction of smartphones, mobile broadband and access dongles which are universal serial bus (USB) modems with SIM card slots to provide internet to a computer. The third wave progressed to fixed-line connectivity through fiber optic technology (Baylon & Antwi-Boasiako, 2016, pp. 1,2). According to the National Communications Authority (NCA) as of January to March 2020, there are 25,479,511 mobile data subscriptions across 4 main mobile network operators (MNOs) in the country (National Communications Authority, 2020). As internet infrastructure expands and internet connectivity becomes cheaper and faster, cyber criminals have more resources to proliferate illegal activity with access to larger pool of potential victims (Baylon & Antwi-Boasiako, 2016). Evidently, telecommunication companies are key custodians of the information and assets involved in perpetration of these crimes.

In response to the increasing threat of cyber-crime activity in the country, the government of Ghana – particularly the Ministry of Communications and its sub-bodies later discussed have

the mandate to make and uphold laws specific to electronic and cyber activity. Laws including the Electronic Transactions Act (Act 772), Ghana National Telecommunications Policy, and the National Communications Act (Act 769) among others, govern the responsibilities of relevant players in the industry (Media Foundation for West Africa, 2017).

Thus, this research is seeking to explore the cyber risk posture of telecommunication companies in Africa, using Vodafone Ghana as a case study.

1.1 Statement of Research Problem

To what extent and in what ways does the risk posture of Vodafone Ghana align with the Ghana National Telecommunications and Cyber Security policy framework?

1.2 Research Questions

Based on the statement of research problem stated above, the study seeks to address the following research questions:

1. What are the cyber risks encountered by telecommunication companies in Ghana?
2. What is the risk management approach of these telecommunication companies?
3. What are the possible risk assessment innovations?
4. What is the cyber risk posture policy evolution of these telecommunication companies?

1.3 Research Objectives

The study will address the following research objectives:

1. To ascertain the cyber risks encountered by telecommunication companies in Ghana.
2. To investigate the risk management approach of these telecommunication companies.

3. To explore the possible risk assessment innovations
4. To examine the cyber risk posture policy evolution of these telecommunication companies

1.4 Scope of study

Vodafone Ghana was chosen as the case study due to its interesting past of evolving from what used to be Ghana's national telecommunications backbone and fully owned by the government of Ghana. The existence of Vodafone Ghana currently partially owned by Vodafone Plc and the government of Ghana was the scope period. As an employee of Vodafone Ghana, I had the privilege of a unique position that allowed me unusual access to data. Thus, making for a convenient and intellectually smart move. However, this privileged position could also limit and constrain ability to talk about some aspects of this study.

1.5 Rationale of study

Through the application of Enterprise Risk Management as the theoretical backbone, this study adds to existing knowledge on the topic and explore how telecommunication companies address cyber risk issues.

1.6 Sources of data

Data was collected using primary and secondary sources. Primary data includes in-depth one-on-one interviews with respondents from relevant institutions to the study. Whereas secondary data includes journals, articles, books, online sites and other relevant documents.

1.7 Method

This study employs the use of a qualitative research approach to understand what kind of cyber threats are peculiar to the telecommunications industry and how these are managed by employing the enterprise risk management conceptual framework.

The chain-link or snowball technique will be used to identify respondents for the purpose of this research. In this technique, information gathering begins with an individual or a few people and then depends on these people to connect the researcher with others who have similar characteristics and can contribute to the research (Lopez & Whitehead, 2013). Identified persons will be engaged in in-depth elite interviews to gather necessary information. Information collection will cease when responses approach a point of saturation – when respondents stop giving new information. This technique is limited in that it relies on referrals from an original list of contacts to identify additional contributors. Thus, participants are often not considered to form a representative enough sample of the overall population under observation (Lopez & Whitehead, 2013).

Data analysis technique required for this study will be content analysis which will involve classifying data purposefully in order to comprehend the data collected and highlight the salient points, insights or findings. Analysis will also use the ERM framework as a guide.

1.8 Literature review: Cyber Security and Risk Management

This section entails a systematic look at the definition of cyber security and its relevance in the perspective of the fourth industrial revolution, the politics of cyber security in developed state, African states and in multinational corporations, and the politics of cyber risk assessment. A conceptual framework based on the concept of enterprise risk management (ERM) will also be discussed.

1.8.1 What is cyber security?

This section discusses the definitions, similarities and differences of information security and cyber security. While both terms are similar and used interchangeably by most, cyber security and information security are not identical (Von Solms & Van Niekerk, 2013). Fundamentally, both practices focus on the protection of sensitive organization data using data security and risk management techniques, yet on closer inspection, cyber security is a broader concept than information security, encompassing additional dimensions.

Information security is "the protection of information resources against unauthorized access" (Raggad, 2010). This indicates that only authorized personnel or ICTs are permitted access to sensitive sources of information sources such as, network, data, software and hardware. This is a definition which clearly pertains to organizational objectives as those form the basis on which authorization decisions are made. Through data abstraction and limitation of access to data sources, authorization is only granted to key business stakeholders who require the information for the execution of specific business objectives. This controlled access to organizational information supports the overall business aim of reducing the likelihood and adverse effects of security incidents.

The ISO/IEC 27000 (2016), a significant global standard, defines information security "as the preservation of confidentiality, integrity and availability of information". These are three aspects of information (Known as 'CIA Triad') that require protection for the attainment of security objectives. Only authorized personnel should be granted access (availability) to the accurately represented information (integrity) without exposure to unauthorized parties (confidentiality) (Harris , 2002). They are also called characteristics of information security. If one of those characteristics is compromised, it is said to be a security failure.

The International Telecommunications Union (ITU) (2008, p. 2) defines cyber security as follows: "Cybersecurity is the collection of tools, policies, security concepts, security

safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets."

This definition emphasizes key elements and subjects under cyber security which require protection. In all instances however, the concepts of "information security and cyber security both aim to maintain the security properties of confidentiality, integrity and availability" (Junp, 2011). However, the ITU's definition highlights a broader perspective of conserving technical and non-technical elements. Von Solms and Van Niekerk (2013) echo this by emphasizing the focus of cyber security in relation to both information and non-information assets within the cyber space or that can be affected via cyber space.

The term cyber security will be used in place of information security as the former covers the broader scope of this research. Thus, the term 'cyber risk management' will be used to connote risk management process that is used to manage cyber risk.

1.8.2 Theoretical Framework: Enterprise Risk Management Theory

This study employs the concept of enterprise risk management (ERM) as the framework and backbone. This section will discuss the connotation and scope of ERM, starting with a fundamental question: "what is ERM?", the shortcomings of the theory, and how it will be operationalized in the context of cyber risk posture of telecommunications in Ghana.

Historically, companies or enterprises have managed risk in a silo manner according to department or division. This is mainly because risks differ according to each section of the business. In this form of risk management, each department has its own tools and practices which appeared fragmented and incongruous. Beginning with Kloman's (1976), "The Risk Management Revolution," many practitioners have advocated a coordinated approach to risk

management (Bromiley, McShane, Nair, & Rustambekov, 2015, p. 266). Kloman described practices in mid 70s and 80s Europe which now form the basis of what is considered to be ERM today. It was a proposal of collective and multidisciplinary risk management rather than isolated and disjointed into several departments. ERM came to the fore as a corporate concept in the mid-1990s and has been defined in several ways according to scholars and collective groups. Dickinson (2001, p. 360) defines ERM as "a systematic and integrated approach to the management of the total risks that a company faces." Casualty Actuarial Society (2003, p. 8) outlines Enterprise Risk Management as "disciplines by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purposes of increasing the organization's short- and long-term value to its stakeholders." Barton et al (2002, p. 4) stipulate that "ERM shifts risk management from a fragmented, ad hoc, narrow approach to an integrated, continuous, and broadly focused approach." Another definition according to Sobel and Reding (2004, p. 29) "is a structured and disciplined approach to help management understand and manage uncertainties and encompasses all business risks using an integrated and holistic approach." The Committee of Sponsoring Organizations (COSO) in (2004) described "ERM as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Therefore, Enterprise Risk Management can be seen as a systematically integrated and discipline approach in managing risks within organizations to ensure firms achieves their objective which is to maximize and create value for their stakeholders.

The spirit of these definitions of ERM will be applied specifically to security risk which typically arises from the usage and operation of information systems. Thus, employing ERM as a conceptual framework, a useful way to operationalize would be along two dimensions: one

is the components of the process of risk management and the other is the manner in which the process is integrated throughout the organization.

The first dimension, the components of risk management is a comprehensive process that requires organizations to define, evaluate, monitor and manage risk. The first step of this risk management process is the definition of risk which involves framing the context of risk-based decision-making and to create a plan to help organizations determine how to assess, respond to, and monitor risk. This includes preempting threats and vulnerabilities, evaluating probability of occurrence and likely impact on subsequent components. It also involves assessing and identifying risk tolerance levels which is the level, types and degrees of risk that are deemed permissible by the organization. Framing risk also comprises strategic executive-level decisions on how risk to organizational activities and assets, individuals, partners, and the Nation, is to be managed by leadership (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 6).

The second component of risk management highlights strategies for evaluation of risk by organizations, within the defined context of risk outlined in the first step. The essence of this step is to identify threats to businesses or threats directed through organizations, internal and external frailties of organizations, potential harm should these vulnerabilities be exploited, and the probability of occurrence of said threats. The business must develop tools and methodologies to assist in this assessment.

The third component of risk management addresses how organizations respond to risk once said risk has been identified in the risk evaluation stage. Following the spirit of ERM definitions earlier, the risk response is to provide congruous, organization-wide action in accordance with the risk frame. This is done by determining appropriate course action consistent with the organization's risk appetite or risk tolerance, and executing responses in accordance with the predetermined courses of action. Types of risk responses that can be

implemented include accepting, avoiding, mitigating, sharing or transferring risk. Appropriate tools and techniques must be developed to assist in responding to risk, evaluating these responses and communicating these responses to relevant stakeholders within and external to the organization.

Finally, the fourth component of risk management outlines ways in which organizations monitor risk over time. This component exists as a check to validate the implementation of risk responses, determine the overall efficacy and pinpoint changes and impacts on the organization.

The process of risk management is flexible and must not necessarily always follow a linear or sequential path through the components elicited above. Information, communication flows as well as execution can be dynamic among the components.

The second dimension of operationalizing ERM, with respect to information security risk, is the manner in which the process is integrated throughout the organization. This is done through an approach with addresses risk at three levels: the organizational level, business processes and objectives level, and information systems level. This approach can be conceptualized as a pyramid with the topmost tier being the organization level, tier 2 in the middle as the mission/business process level and tier 3, the base of the pyramid, as the information systems level (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 9). This multitier approach enables seamless communication and execution of the risk management process across the total organization through inter-tier and intra-tier interaction.

Tier 1 tackles risk from the perspective of the organization and implements the activities of risk framing which involves providing context for all the organization's risk management activities. Governance structures consistent with the strategic goals and objectives of the organization must be established to give insight into conducted risk management activities. These governance structures include the implementation and establishment of a risk function,

a risk management strategy which reflects risk tolerance, and the definition and implementation of organization-wide strategies for investment in resources, tools and techniques for information security. Missions and business divisions outlined in this tier significantly impact the design and development of the processes in Tier 2 to achieve these functions which trickles down into how information systems are allocated and deployed at Tier 3.

Tier 2 addresses risk from the perspective of business processes and is based primarily on the risk context, decisions, and activities at Tier 1. These activities include defining processes to support mission and business functions identified in Tier 1, prioritizing these processes according to criticality and sensitivity of information required, incorporating information security requirements into the process and establishing an information security embedded organization architecture. All of which are aligned with the strategic organizational objectives. Tier 2 influences and guides deployment of security controls to information systems at Tier 3. This level also provides feedback to Tier 1 which could result in modification of the organization's risk frame and management activities.

Tier 3 approaches the subject of risk from the perspective of information systems and is based on the risk context, decisions and activities highlighted in the previous two tiers. Risk management activities in this tier comprise of the categorization of organizational information systems, assignment of organizational information systems security controls and the ecosystems under which those information systems operate. These are consistent with the established enterprise architecture and information security architecture of the organization, managing the selection, operation, evaluation, accessibility to, and monitoring of allocated safety features, forming parts of a well-structured system in the development life-cycle process executed across the organization (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 10). These activities also provide essential feedback to Tiers 1 and 2.

Scholarly reviews and critique of this concept and surveys among risk managers reveal that several articles define extensively the features and functions of the ERM process, with only a few providing guidance on how to achieve it. Practically all literature do not address the challenging combination of cultural, logistical and historical issues that have plagued and are unique to all organizations. Many articles use great overarching statements that are quite broad, vague and all-encompassing. There exists a clearly identifiable gap in the availability of information on ways through which the organizational silos can be harmonized to truly transform traditional risk management. Implemented systems or tools for ERM depend on the type of unique risks faced by organizations thus it is impossible for a general ERM system suitable for any kind of organization (Kerstin, Simone, Nicole, & Lehner, 2014, p. 13). Lastly, the impact of corporate culture on ERM execution and practices is inadequately addressed in the literature (Fraser, Schoening-Thiessen, & Simkins, 2011, pp. 399-401).

1.8.2.1 Cyber security risk management

Measures that organizations put in place to protect valuable company assets constitutes cyber security risk management (Testrig, n.d.). Risk management enables effective decision making and communication of results within the organization (Kure, Islam, & Razzaque, 2018, p. 2).

Literature on handling of information system and computer related security risk generally focuses on technical issues and disregards application of some aspects of the risk management process (Eling, McShane, & Nyugen, 2021, p. 96) There tends to be more focus on "reducing probability of an adverse event than on reducing its consequences" (Blakley, McDermott, & Geer, 2001, p. 99). Collier et al. (2013, p. 469) notes that focuses on "technical issues at component levels" such as threat and vulnerability detection should shift towards a more holistic analysis that integrates the physical, information, cognitive and social domains – the four domains of cybersecurity. The first domain, physical, refers to the hardware, software and

networks that make up cyber infrastructure. Information domain, the second, feature "monitoring, information storage and visualization" (Collier, Linkov, & Lambert, 2013, p. 469). The third, cognitive domain, implores proper analysis and sensing of information that influences decision making. Finally, the social domain focuses on consistency of cyber security decisions with "social, ethical and other considerations that are characteristic of their enveloping societal domain" (Collier, Linkov, & Lambert, 2013, p. 470).

Cyber risk management process involves identification, analysis, and treatment. A method of identifying cyber risks is whether they affect the 'CIA triad' – confidentiality, integrity and availability (Biener, Eling, & Wirfs, 2015). These three in addition to authenticity (validity of transmission) and non-repudiation (proof of identity and delivery) are termed the five (5) pillars of cyber security (Infinit-O, 2018). Howard and Longstaff (1998, p. 14) note that "vulnerability arises in different stages of development" - design, implementation and configuration.

Cyber risk analysis looks at factors that could increase a firm's chances of experiencing cyber-attacks, tools and methods in analyzing the probabilities as well as impacts of cyber-related events. Organization characteristics such as the firm size, corporate social responsibility activities, and financial strength are determinants in their chances of experiencing cyber-related events. Firm size implies the quality and breadth of infrastructure. On one hand, smaller organizations that have less robust infrastructure in comparison to larger firms could experience more cyber-attacks. On another hand, larger firms are likely to hold more data thus are bigger targets. However, Lending et al (2018) notes that due to the better information security infrastructure of larger firms, cybercriminals are discouraged from attacking. The way in which an organization's activities may affect the environment, the level of involvement in community and the overall social responsibility can be a factor in why cybercriminals target firms. Largely socially irresponsible organizations are likely to be targeted by activist hackers as a form of punishment (Eling, McShane, & Nyugen, 2021). Finally, a firm's financial strength

which dictates the investment in cybersecurity systems has a play in probability as well. Financially strong organizations are less likely to experience cyber-attacks.

Tools and methods used to assess probabilities include risk scoring based techniques (Shetty, et al., 2018), software that use statistical analysis, adversarial risk analysis (Insua, et al., 2019) and machine learning techniques (Sentuna et al., (2020).

Cyber-related events have impacts on shareholder value and reaction, consumers, reputation and compliance with legal and regulatory obligations. Shareholder value is negatively affected in the event of cyber-attacks. These threats "incur additional costs for targeted firms, which lowers their long-term performance on average" (Eling, McShane, & Nyugen, 2021, p. 103). Reactions of shareholders to cyber-related events tend to waver based on frequency – on the onset of cyber incidents there are high negative shareholder reactions but as the frequency of events increase, reactions from shareholders plateau as they become familiar with the frequent incidence. Consumer trust and spend is affected by organization's that experience cyber-attacks. Occurrence of breaches negatively impacts the trust consumers have in a business thus affect the money they are willing to give away to the business (Bansal & Zahedi, 2015). The organization's reputation erodes, and this further affects the bottom line. Legal and regulatory impact can be in the form of fines and sanctions as laws.

Cyber risk treatment is determined by a combination of the likelihood and level of impact of a cyber-related event. Treatment includes "avoidance, mitigation to reduce likelihood and/or impact, transfer, and retention" (Eling, McShane, & Nyugen, 2021, p. 104). Although recognized as a treatment option in literature, avoidance is reflected on as unrealistic as in this age of dependency on information technology and digital era of industry 4.0, organizations and consumers always expect to be secure. Thus, management of the risk is seen through the other treatments. Mitigation of cyber risks include measures that protect the five pillars of

cybersecurity (confidentiality, integrity, availability, authenticity, and non-repudiation). Examples of these measures are password and biometric authentication, virtual private networks, and encryption. Risk transfer relies on insurance as a measure. Cyber insurance policies coverage includes liability areas such as network security, privacy, communication and media, and cyber extortion (R & R Insurance). Retention of risk is when the best effort of mitigation and transfer yields a level of residual risk that is acceptable (Eling, McShane, & Nyugen, 2021).

Stine et al. (2020) notes that there is difficulty in integrating cybersecurity programs into the framework of ERM. As discussed earlier, ERM is a holistic approach to risk management – implemented across all levels of the organization. However, due to the complexity in defining cyber risks, it tends to be treated in a silo. Weill and Ross (2004)stipulate that although cyber risk is and should be seen as important in all levels of corporate governance, "most boards continue to ignore or delegate technology matters to management, sometimes several layers down the organization structure" (Valentine, 2016, p. 179).

1.8.3 Cyber Security: The Fourth Industrial Revolution in Perspective

Industrial revolutions are important milestones that have changed the course of human history. In the 18th century, the invention of steam power resulting in mechanization and mechanical power generation marked the beginning of the first industrial revolution (Rojko, 2017, p. 79). The second industrial revolution introduced electric energy-driven mass production, which empowered factory workers to easily and quickly replicate products with the help of assembly line techniques. The third industrial revolution, the beginning of the information age, was characterized by the onset of electronics and the automation of processes using computers, resulting in a highly productive industrial era (Frost & Sullivan, 2017, p. 3). Presently on the fourth industrial revolution, also known as 'Industry 4.0', the world is witnessing rapid

advances in technology and a new age of integrated digital or cyber space and physical space catalyzed by the Internet of Things (IoT). Industry 4.0 involves processing enormous data volumes, engineering human-computer interactive systems and improving communication between the digital and physical environments (Frost & Sullivan, 2017, p. 4).

The concept of industrialization is not limited just to production systems but also includes the complete value chain (from producers to the consumers of one enterprise towards the 'Connected Word' of all enterprises) and the functions and services of all enterprises (Rojko, 2017, p. 86). "The main idea of Industry 4.0 is to exploit the potentials of new technologies and concepts such as availability and use of the internet and IoT, integration of technical processes and business processes in companies, digital mapping and virtualization of the real world, and 'smart' factory including 'smart' means of industrial production and 'smart' products" (Rojko, 2017, p. 80). The onset of this new industrial age has changed conventional terms like production planning and control to cyber-physical systems and IoT, and data management to Big Data, Cloud and Cybersecurity. Organizations adapting to these new technologies rely on efficiency of their information systems to facilitate their business activities. These 'smart' and interconnected organizational systems not only create more opportunities but significantly increase the exposure to many security risks, with critical and financial impacts (Pereira, Barreto, & Amaral, 2017, p. 1257).

Cybersecurity in the industrial landscape gained momentum after the infamous Stuxnet attack in an Iranian nuclear facility in 2010 (Frost & Sullivan, 2017, p. 9). The mysterious attack at the time, deemed the world's first digital weapon, sabotaged and wreaked physical havoc on centrifuges from carefully placed malicious files on computer systems. The trajectory of evolution of cyber-attacks since 1980s to the present 21st century has moved from general attacks which are less complex and sophisticated like password cracking or password guessing, to very complex and highly sophisticated security threats like enterprise cyber-espionage,

malicious codes, Denial-of-Service (DoS), and supply chain hacking (Ervural & Ervural, 2018).

Moving towards Industry 4.0 is an enormous endeavor which directly impacts in several areas of today's manufacturing industry, particularly in security. It is essential, and urgent, that organizations embrace the development of a strategy to deploy and run security compliance processes that Industry 4.0 requires, especially towards reducing the organizational level of exposition as well as to proper manage the mitigation procedure of its impacts (Pereira, Barreto, & Amaral, 2017, p. 1259).

1.8.3.1 Telecommunications Industry Security Threats

Telecommunication companies constitute some of the biggest targets for cyber-attacks due to their operation and control of critical infrastructure which facilitate the storage and flow of copious amounts of highly sensitive data. This section deals with commonly identified security threats peculiar to the mobile telecommunications industry.

1.8.1.3.1 Denial-of-service (DoS)/ Distributed denial-of-service (DDoS) Attacks

Denial-of-Service (DoS), also known as a Distributed Denial of Service (DDoS), is the process of halting the operations of a system or application, rendering it unavailable and unusable (DDoS attack statistics: A look at the most recent and largest DDoS attacks, 2020). This form of cyber-attack typically involves flooding the targeted device with traffic from one computer and internet connection. Distributed denial-of-service (DDoS) attacks, as the name suggests, flood applications or systems of victims with traffic from multiple sources. These multiple sources are also known as bots or botnets. DDoS attacks are challenging to get a handle on as it is difficult to pinpoint the exact origin of the attack. During the period where the system of the victim is overwhelmed with unusually large volumes of requests, legitimate customers of

the victim are unable to access relevant information systems and network sources. The damage caused by DoS/DDoS cyberattack can incur very high costs for an organization resulting in possible material damage to servers and networks, operational, financial loss as well as reputational damage. Data from Bulletproof's 2019 Annual Cyber Security Report indicates that a small company could lose up to $120,000 if they fall victim to a DoS or DDoS attack. For larger companies, costs could surpass $2 million (Bulletproof, 2019). According to a report by NetScout, in 2019, there were 8.4 million DDoS attacks targeted at IT infrastructures, cloud, mobile networks and IoT devices (NetScout, 2019).

1.8.1.3.2 Supply Chain Threats

The connected nature of Industry 4.0 increases the potential to make supply chains more efficient. The reliance of mobile operators on numerous external parties for the delivery of key operational infrastructure, products and services, extends to their customers who in turn depend on these operators for the facilitation of different life and business activities. This complex chain of dependency opens up all parties of the downstream links to risks and vulnerability of suppliers, thus, making the supply chain increasingly attractive to attackers (GSMA, 2019). In this supply chain of interconnectedness, cyber attackers do not need to target the main entity to compromise their security. They can focus on weak points in the supply chain to compromise which will eventually affect the target. Thus, threat lies in who organizations do business with and where materials needed to achieve mission and business objectives are sourced from. An inefficient management of the supply chain exposes the operator to possible erosion of brand and trust, regulatory sanctions and significant financial losses.

1.8.1.3.3 Human-related Threats

Internal human risk threats include actors of malicious intent as much as negligence. GSMA (2019) outlines four types of human-related threats: social engineering and phishing attacks,

misconfiguration, disregarding processes and insider threat. Social engineering attacks are when the attacker influences the user to take a desired action which comprises their security. Phishing a method of social engineering aimed at the theft of sensitive user information including login credentials and digital banking accesses. Usually, the attacker masquerades as a trustworthy entity and deceives the victim into taking an action such as opening an email link, which compromises their security. These malicious links typically lead to the installation of malware which may spy on their online activity or freeze their system till they pay a ransom (Imperva, n.d.). "Misconfiguration, often dubbed the 'fat finger attack', is where devices are left in an insecure default state or configured insecurely by mistake. This is then leveraged by an attacker" (GSMA, 2019, p. 15). The third type of human-related threat is disregarded processes. This is when processes are often outlined but not followed. Often when a process is deemed laborious or unnecessary. Finally, insider threats, which is when someone with insider knowledge of how an organization operates intentionally acts in a malicious way (GSMA, 2019). Some insiders help voluntarily, others are coerced through blackmail.

1.8.1.3.4 Internet of Things (IoT) Devices

The Internet of Things (IoT) has been welcomed by consumers and enterprise. Majority of IoT attacks exploit poorly configured factory settings of devices. Many IoT devices are built using low-end, cheaply manufactured components and are sold in large volumes, making them ideal for reaching many victims at a time. The attacks of users of these devices also exposes the telecom operators' networks to the same security risks, potentially harming their business operations.

1.8.4 The Politics of Cyber Security

The notion of security has different meanings in the realm of international relations. The meaning is interpreted and covers relevant spaces according to era. In the World War II and Cold War eras, international security revolved around military power or use of force and focused on superpower conflict and nuclear war. The concept of international security also included food, energy supplies, ideology, science and technology, environmental degradation, health and human security (Tsakanyan, 2017, p. 339). At the end of this era, the scope of international security "had to be recast to reflect the changing nature of conflict" (Freedman, 1998, p. 48). Increased access to the internet in 1990s brought introduced a cyber space that would also redefine the traditional and conventional notions of security. Cyberspace enables people and communities interact, socialize and organize all around the globe. Its vast capabilities and applications posed national and international concern. It created opportunity for exploit by criminals and even state governments. Increasing cyber incidents have given the impression that cyber-attacks are becoming more targeted, more expensive, more disruptive, and in many cases more political and strategic (Cavelty & Wenger, 2019, p. 1). Protecting this cyber space, ensuring cyber security, is a need that is increasingly growing in the realm of diplomacy and world politics.

The definition of cybersecurity is contested politically in both national and international arenas. The concept keeps evolving from being discussed as merely information security in small expert and technical circles to a matter of national security dealt with strategically in the highest government circles. It is contested among state actors as there is discord in agreement on common vocabulary (Giles & Hagstead, 2013, p. 1). According to Cavelty and Wenger (2019), cyber security politics is characterized by two main factors – "The first is use and misuse of digital technologies by human actors in economic, social and political contexts. The second is conflicting settings of formal and informal negotiations which define responsibilities, legal frameworks and acceptable rules of engagement among the state, its people, and the private

sector." Through their use, technologies can be seen as material objects, power resources or neutral tools that drive social change (Hoijtink & Leese, 2019). Contrarily, technologies can be seen as stages on which the operation of power relations are highlighted and where the shaping of the behavior of social and political actors occurs (Behrent, 2013, p. 57). Makers of technologies infuse their intentions, norms and values when designing and the products use is manipulated according to existing power structures. Thus, "technologies are shaped by political ideas and power structures and shape the possibilities of political action in turn" (Cavelty & Wenger, 2019, p. 6).

Technologies and cyber space have given rise to 'new power' and threats that are even recognized as a 'fifth domain' after land, sea, air and space (The Economist, 2010). Cyber power is the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. It is understood as exploitation of cyberspace resources for the attainment of specific political objectives in and out of cyberspace (Nye, 2010, p. 4). This new power however, has its own dependencies and vulnerabilities (Rattray, 2001).

Actors in cyberspace and cybersecurity can be the state and non-state actors which include individuals, private corporations, and interest groups. However, to be categorized as "an actor in cyberspace, the following three qualifications of 'actorhood' should be met; structural, population and territorial elements" (Seunghwan, Birch, & Bengtsson, 2016, p. 219). Structural elements include skilled human resources performing duties as system developers and administrators with capability of identifying vulnerabilities, and access to robust equipment and infrastructure. Population elements include both technical and consumer users of cyber systems. More users mean more information in systems which translates into more power for the actor. The last criteria is the territorial element which includes "ownership and access rights to user information, user-contributed content, and all types of core data. The level of access to

user data defines the size of an actor's cyber territory" (Seunghwan, Birch, & Bengtsson, 2016, p. 220).

1.8.4.1 Politics of Cyber Security in International Relations

Cybersecurity can be seen as an instrument to achieve a state's national interest. It can also be used as an instrument to influence the views and opinions of adversaries. This philosophy and operationalization are seen in approaches of states like the Unites States, Russia and China and is manifested in the play of world politics. This section explores the role of cybersecurity in global politics with a keen examination of the approaches of the USA, Russia and China and how these approaches interplay in relationships between them.

The United States, leaders in the ICT industry, is among the first countries to directly experience the negative impact of the information revolution (Tsakanyan, 2017, p. 342). There is heavy reliance on network technologies and information infrastructure to ensure the proper functioning sectors of a country's economy and the lives of its citizens, including health care, transport, finance and agriculture. The Federal Bureau of Investigation (FBI), according to Tsakanyan in *The role of cybersecurity in world politics*, highlights three key groups of actors that pose threats in cyberspace. These are organized crime syndicates who mostly target financial services, state sponsors who engage in cyber espionage against enterprises and public institutions, and terrorist groups who orchestrate disparaging activities against a country's critical information systems infrastructure, thus, posing a national security threat.

Viewing cybersecurity as a core component of national security, the Chinese government holds this issue in high regard. They are cautious of software and infrastructure from Western manufacturers and perceive its use as a threat to national security. This view manifests in the growing power China continues to garner by expanding their territory in IT products and services (Tsakanyan, 2017, p. 345).

The Russian approach, through the lens of their national interests, views cyberspace as a tool to weaken the socio-political and economic systems of other states, psychologically threaten populations, destabilize society and compromise the flow and authenticity of the information space of other nations (Tsakanyan, 2017, p. 346).

Kshetri (2014) further deals with approaches of these select countries in relation to cooperation on formal treaties and frameworks for cybersecurity in his work Cybersecurity and International Relations: The U.S. Engagement with China and Russia. He first notes that alliances and policy guidelines involving treaties are sustained only when there is a sense of mutual advantage. This presence of mutual advantage is the first determinant to joining an international coalition. Case in point, referencing Goldsmith (2011, p. 3) and Keyser (2003), the Council of Europe (CoE) treaty, the most popular cybercrime treaty, have clauses that promote intrusion of national sovereignty which present no incentive to China, Russia and many developing countries.

He goes on to question whether informal approaches of international alliance perform better than formal ones in dealing with international cyberspace problems. The U.S. and Russia have differing approaches. U.S favors cooperation through ad hoc or informal mechanisms that tend to bypass formal institutions and treaties, whereas Russia favors international treaties to secure cyberspace against threats. Citing Lipson (1991, p. 500), it is of the positive view that informal approaches have notable impact as they are more flexible that treaties. A positive playout of this is the formation of trans-governmental networks sharing information with each other, harmonizing guidelines and best practices. These informal networks are arguably "the optimal form of organization for the Information Age" (Kshetri, 2014, p. 8)

Kshetri goes on to analyze relationships between the aforementioned countries concerning issues of cyberspace. First between the U.S. and China, there is an air of mistrust and disharmony in cooperation. Allegations and counter-allegation characterize this relationship in

cybersecurity (Kshetri, 2014, p. 11). China has been accused of consistently engaging freelance hacking groups in international cybersecurity attacks, thus providing "plausible deniability" about any association with the state. Despite not having concrete evidence clearly showing involvement, the allegations are relentless based on noticeable patterns and circumstantial evidence. The Chinese response to these allegations are strong denial and accusation of lackluster attitude in western counterparts when it comes to fighting cybercrime.

This relationship is further emphasized in challenges of technology companies of both sides operating in either territories. For example, the Chinese government are wary of companies like Microsoft, and the U.S. government are wary of Huawei. Huawei, the world's biggest seller of network telecommunications equipment, is seen in controversial light (Vaswani, 2019). Given the status of 'national champion' in China due to its successful local and international sales, strategic contributions to the Chinese government and powerful political connections, this pioneer of ICT and telecommunications is accused of being a gateway spy on Western nations.

The seeds of suspicion stem from events such as the compromise of the Chinese- built African Union (AU) headquarters in Addis Ababa. Completed in 2012, everything was custom-built by the Chinese- including a state-of-the-art computer system. In 2018, a French newspaper reported that AU's computer system had been compromised, with data from AU servers transferred to servers in Shanghai for five years. "It was also reported that microphones and listening devices had been discovered in the walls and desks of the building following a sweep for bugs" (Vaswani, 2019). The main supplier of information and communication technology systems to the AU headquarters was China's best-known telecoms equipment company - Huawei. However, just because Huawei supplied equipment did not mean it was complicit to any theft of data. There was also no evidence to indicate that Huawei's telecoms network

equipment was ever used by the Chinese government - or anyone else - to gain access to the data of their customers. Regardless, these reports bolster the suspicions around the tech giant.

In 2018 amidst a trade war between the United States and China, Huawei became entangled in the string of events deepening suspicions of Western nations and affecting diplomatic relations. Huawei's chief financial officer and founder's daughter, Meng Wanzhou, was arrested in Canada at the request of the US, who accused her of breaking sanctions against Iran, and attempted theft of trade secrets.

The US sees the company as a strategic arm of the Chinese Communist Party. With the trajectory of telecommunications evolving into 'fifth generation' or 5G, which promises faster download speeds and much greater connectivity between devices than at present, Huawei is one of the companies best placed to lead the evolution. The US began to warn nations against the use of Huawei technologies. "In 2019, U.S. Secretary of State Mike Pompeo warned that the United States would not be able to partner with or share information with countries that adopt Huawei Technologies Co Ltd systems, citing security concerns. Pompeo said nations in Europe and elsewhere need to understand the risks of implementing Huawei's telecommunications equipment and that when they did, they would ultimately not use the company's systems" (Reuters, 2019). In an interview on the subject, Pompeo said, "If a country adopts this and puts it in some of their critical information systems, we won't be able to share information with them, we won't be able to work alongside them." This resulted in the US adding Huawei to a list of companies that American firms cannot trade with unless they have a licence (BBC News, 2019).

Scrutiny of cybersecurity between the two nations expands into the realm of social media as well. Chinese-owned applications such as TikTok and WeChat are in danger of being banned in the US for suspicions of threat against national security and prevention of Beijing from

exploiting the apps to collect user data or disseminate propaganda (Whalen, Lerman, & Nakashima, 2020).

Thus, technology and cyber security remain entangled in relations between the two nations.

U.S. – Russia relations on issues involving cyberspace are in disharmony in a way that further emphasizes historical relations from the Cold War era. Illustrated in several examples, points of disharmony include absence of notifying either side when action is to be taken on criminal nationals of each side.

From the national security and international relations standpoint, there are a number of unique aspects of the cyberspace which may offer some insight into the nature of relations among nations as noted above. Firstly, "the nature of cyberspace makes it impossible to trace the actual origin of the software" (Choucri & Goldsmith, 2012, p. 71). Thus accusing a state or entity of foul play would be based on inferences of circumstantial evidence rather than direct, factual and conclusive evidence. This unique characteristic leads to the second which is that offenders in cyberspace are more emboldened as compared to physical space. Lastly, citing Lipson (1991) and Ramseyer (1991), Kshetri notes that cyber violators are very rarely punished thus actors are likely to engage in violations if such violations cannot be witnessed and violators go unpunished.

1.8.4.2 Politics of Cyber Security: African States

In Kshetri's work on *Cybercrime and Cybersecurity in Africa, "*he notes that cybersecurity is considered to be as a luxury, not a necessity in many African economies. Its importance has not yet been sufficiently appreciated or acknowledged in the continent" (Kshetri, 2019, p. 78). "The African Union Commission and Symantec, as part of the Global Forum for Cybersecurity Expertise (GFCE) Initiative, released a report analyzing cyber security trends and government responses across Africa. It focused on 5 key areas: social media, scams, and Email threats, smartphones and the Internet of Things, business email Scams, rise of ransomware and

cryptolocker and vulnerabilities" (Cyber security trends and government responses in Africa, n.d.). Increasing access to smartphones and increased connectivity make the emerging economies in Africa attractive targets for cybercrimes. The report found out that of 54 countries in Africa, 30 lacked specific legal provisions to fight cybercrime and utilize electronic evidence (Mathe, 2019). In 2017, cybercrime cost Africa an estimated total of $3.5 billion (Mathe, 2019). Annual losses to cybercrimes in the same year in Nigeria and Kenya were $649 million and $210 million respectively. South Africa loses $157 million annually to cyberattacks (Kshetri, 2019, p. 77). Further noting that "the sectors in which cybercrime is predominantly active are Banking/Financial services, government, e-commerce platforms, mobile payments and telecommunications."

Problems that the continent faces include vulnerable systems, lax cybersecurity practices, a lack of skills among internet users to protect themselves from rapidly rising cyber-threats, severe shortage of cybersecurity manpower and weak legislation and law enforcement. Despite these, measures strengthening cyber readiness, legislation and enforcement are gradually improving.

Conventions, treaties and Memorandum of Understanding (MoU) specific to the African region exist to enable more effective cooperation on Cybersecurity initiatives. Such include a MoU between the Economic Community of West African States (ECOWAS) and International Telecommunications Union (ITU), and the African Union Convention on Cyber Security and Personal Data Protection.

Signed on the 8th of June 2015, the MoU between the ECOWAS and ITU serves as a non-binding framework for collaboration between the Parties, within the framework of the ITU Global Cybersecurity Agenda and in accordance with the parties' commonly agreed goals for a more secure and safer information society and on the basis of mutual benefit (ITU, n.d.). Common interests and mutually agreed points of cooperation include elaboration of regional

Cybersecurity initiatives through ECOWAS and enhancing the Cybersecurity posture of ECOWAS member countries through country specific initiatives including:

- The National Computer Incident Response Team (CIRT)/ Computer Emergency Response Team (CERT) programme whereby constant evaluations and assessments, including regional cyber drills, are conducted;
- Improving Cybersecurity efforts in ECOWAS nations through custom-made capacity building initiatives and collaborative roadmaps executed in agreed phases;
- the Global Cybersecurity Index which evaluates the Cybersecurity competencies of member nations, allowing for timely Cybersecurity measures and the fostering of a globally consistent culture of Cybersecurity;
- the Child Online Protection initiative, an international collaborative network with the sole aim of advancing the protection of children and young people online globally through the provision of guidance on safe online conduct.
- The synchronization and improvement of laws that pertain to effectively addressing the prosecution of Cybercriminals;
- the communication of national Cybersecurity policies which detail the creation and execution of national frameworks for Cybersecurity and critical information infrastructure protection (CIIP) through a comprehensive approach.

1.8.4.3 Politics of Cyber Security: Multinational corporations

The activities of multinationals challenge the traditional role of the state in security, and in this context, cybersecurity as well. Through innovation, multinationals are able to amass significant cyber power and cause power shifts (Seunghwan, Birch, & Bengtsson, 2016, p. 225). Thus, through activities not constrained by boarders, access to robust systems, infrastructure and expertise, large number of users and the non-obligatory show of good intention towards these

users, companies could be more powerful than states in the realm of cyberspace. A clear example of these powerful companies are Google, Apple and Microsoft. In Sigholm's work in *Non-State actors in cyberspace operations,* it is noted that although corporations are perceived as law-abiding entities, they are sometimes caught up in matters of cyberwarfare. This is "at the request of a nation state, either by being on a government contract or by more autonomous actions under the government's blessing" (Sigholm, 2013, p. 21). Intelligence agencies may also use corporate fronts as a cover for cyber espionage operations. Large international corporations doing business in many different countries may find themselves in a precarious situation during a cyber-conflict, finding themselves on both sides of the front line.

1.8.4.3.1 Public–Private Partnership in National Cyber-Security Strategy

Public-private partnerships (PPP) are used as a means to address both non-traditional and traditional security threats. However, in the context of national cyber security, the relationship is uniquely problematic (Carr, 2016). There is lack of clarity in the roles and priorities of both sides which is characterized by reluctance of politicians of the state to claim authority for introduction of tougher cyber laws, and the private sector's aversion to accepting responsibility or liability for national security. Authors such as Dunn Cavelty and Suter (2009) explore the role of and capacity of government in PPP for protection of critical infrastructure. Their article, *Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection*, develops a comprehensive understanding of how policy-makers and the private sector are conceptualizing their respective roles in national cyber security, where there may be disparity in these conceptions and what implications this may have for national and international cyber security. This dynamic in application to the case study at hand, Vodafone Ghana (representing the private sector) and Government of Ghana (representing the public), could be examined for their points of contradictions in terms of what is of priority to both sides and how it conflicts. The interests of private businesses and that of the state are often

not convergent when it comes to Critical Infrastructure Protection (CIP) (Dunn Cavelty & Suter, 2009, p. 3).

Points of divergence include the following arguments. Firstly, the degree of attention to confidentiality might not be the same on both sides thus information transfer from private to public entities could cause risk such as reputational damage to the private entity. Additionally, from the government perspective, accidental or intentional divulging of classified information may also hamper activities of intelligence services and other institutions. Secondly, majority of companies which are multinationals or transnational companies subject themselves to higher international standards thus are "only partially appreciative of the necessity of national cooperation" (Dunn Cavelty & Suter, 2009, p. 3). Thirdly, the private sector views the issue from the perspective of business administration and business continuity thus is not treated with the same level of urgency. Fourthly in *The Private Sector: A Reluctant Partner in Cybersecurity*, Etzioni (2014) notes that despite corporations being considered as rational actors thus expected to voluntarily take measures to protect themselves and realize profits, CEOs have been shown to focus on short-term costs and benefits, to the detriment of longer-term effects. This translates into underinvestment in controls and measures to address cyber security. Fifthly, expanding the issue of bottom-line and realizing profits, obligatory cybersecurity regulations would impose substantial costs on private sector thus impeding profitable operations. Companied would need to spend millions in order to develop cybersecurity systems. Lastly, further emphasizing the extent of roles in the policy-making of cyber security and the extent of divergence, opponents of government cybersecurity regulations claim that government mandates will actually hamper cybersecurity and other innovations in the private sector (Etzioni, 2014). Establishing clear standards for companies would impede their flexibility by forcing them to introduce cumbersome or inefficient cybersecurity measures. "PPPs require a complementarity of goals, mutual trust, clear goals and strategies,

clear distribution of risks, clear sharing of responsibilities and authority, and market and success-oriented thinking to be strategically" efficacious (Dunn Cavelty & Suter, 2009, p. 3).

1.8.5 Cyber Security Conventions and Treaties: The African Union Convention on Cyber Security and Personal Data Protection and the Budapest Convention in Perspective

This section deals with treaties and conventions on cybercrime that Ghana has ratified.

In June 2014, the 23rd Ordinary Session of the Summit of the African Union held in Malabo, Equatorial Guinea, adopted the legal instrument; the African Union Convention on Cyber Security and Personal Data Protection (African Union, 2014). This is also known as the Malabo Convention. The Convention covers a very wide range of online activities, including electronic commerce, data protection, and cybercrime, with a special focus on racism, xenophobia, child pornography, and national cybersecurity (African Union adopts framework on cyber security and data protection, 2014). Out of 55 states, 14 have signed on to the Convention, 8 have ratified/acceded and 8 have deposited (African Union, 2020). The treaty will enter into force 30 days after the 15th instrument of ratification or accession is deposited (African Union, n.d.).

Officially known as the Council of Europe Convention on Cybercrime, the Budapest Convention was the first international treaty to focus explicitly on cybercrime (Daskal & Kennedy-Mayo, 2020). Entering into force in 2004, the convention focuses "on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation" (Council of Europe, n.d.). It serves as a

guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State Parties to this treaty.

On December 3rd 2018, the Republic of Ghana deposited the instruments of accession to the Budapest Convention on Cybercrime (Council of Europe, 2018).

1.9 Arrangement of chapters

This study is divided into 4 chapters. Chapter one will include the general introduction to the study with a thorough literature review on the subject. Chapter two will delve deeper into the significance of cyber security in the international arena. Chapter three will assess the cyber risk posture of Vodafone Ghana using the chosen conceptual framework. Chapter four will involve the summary of Research Findings, Conclusion and Recommendations.

CHAPTER 2
Vodafone and Ghana's National Telecommunications Policy

2.0 The evolutionary history of Vodafone in Ghana

Vodafone in Ghana is an operating company of Vodafone Group Plc – a mobile telecommunications company, with a significant presence in Europe, the Middle East, Africa, Asia Pacific and the United States (Vodafone Ghana, 2020). The range of communications solutions include mobile, fixed lines, internet, voice and data. The company also provides M-Pesa, locally known as Vodafone Cash, "a mobile money transfer and payment service that enables customers to access their bank accounts to send and receive money, purchase goods, pay bills, and save money and receive short-term loans" (Vodafone, n.d.).

Vodafone Ghana, originally the Post and Telecommunications Department of the Colonial Administration, went through several transformations before being renamed Ghana Telecom in 1996 (Ajao, 2009). The Telecommunications Division of the Department turned Corporation in 1974, was carved out in 1993 (Ghana Post, 2020). Then, the state-owned corporation had almost full monopoly over all telecommunication services (Haggarty, Shirley, & Wallsten, 2002, p. 4). However, due to a history of poor service characterized by lack of access, poor quality for those who had access, high international tariffs, inefficiency and poor management, as well as other contributing institutional factors, the incumbent was unpopular and this led to reform in the telecommunications sector (Haggarty, Shirley, & Wallsten, 2002, p. 4). In the process of reform, a road map document called the Accelerated Development Program (ADP) subsequently launched in 1994 (Osei-Owusu, 2017, p. 54). The primary means to achieve the above policies and objectives documented in ADP was the establishment Ghana Telecom (in June 1995). This was to replace the then telecommunications division of the Post and Telecommunication Operator. The implementation of the ADP was expected to pave the way for the denationalization and total liberalization of the telecom industry. Upon privatization in

1996, Ghana Telecom was divested first to a consortium called G-Comm Limited led by Telekom Malaysia and was later managed by a Norwegian management services company known as Telenor Management Partners (Ajao, 2009). In 2006 after taking possession of 100% shares of Ghana Telecom, the Government took a decision to partially privatize the company. The initial objective was to sell 66.67% shares of the fully owned company to a strategic investor in order to attract private sector capital and technical expertise in the country's telecom sector (Agyekum, 2010). A bidding process was launched to invite interested parties. The process culminated in August 2008 with a $900 million payment by Britain's Vodafone Group Plc for a 70 percent stake in Ghana Telecom leaving 30 percent for the Government of Ghana (Ellott & Kpodo, 2008).

2.1 Telecommunications Policy in Ghana

Telecommunications is one aspect of a wider trend of technological and market convergence which encompasses fields such as broadcasting, information technology, and electronic commerce. The Government of the Republic of Ghana recognizes its importance and has thus put in efforts to be at the forefront of the information and communications revolution in Africa (Government of Ghana, 2004). These efforts include liberalization of basic telecommunications services by embracing the potential of competitive markets and introducing reform to the sector. Thus, transforming the telecommunications industry from a largely monopolized, state-owned model to a broadly competitive, private and open market model.

2.1.1 International telecommunications Segment

In the international market sphere, telecommunications infrastructure and operations carry communication signals across Ghana's borders. Elements of this segment include licensed

gateway operators (operators who have been officially authorized to maintain connection for international terminations), South Atlantic Telecommunications cable no. 3 (SAT-3) access (a submarine cable which connects West Africa, South Africa to Europe), private licensed Very Small Aperture Terminal (VSAT) systems (licensed access to international data networks by private users), and unlicensed international bypass services (unauthorized service providers who through sidestepping channels of licensed international operators, connect international voice calls to the local public network) (Government of Ghana, 2004).

2.1.2 Domestic public telephone services

These services provide telephone connectivity within Ghana. Components of this segment include fixed wire line networks for basic telephone services, wireless mobile networks through the use of defined frequencies, and public telephones and tele-centers allowing calls and charging per use (Government of Ghana, 2004).

2.1.3 Dedicated transmission networks

These networks are responsible for providing connection between two or more dedicated locations. This segment can also be leveraged as wholesale services to licensed retail operators, private entities for closed user group services or for public signal distribution enabling services such as TV connectivity and broadband (Government of Ghana, 2004).

2.1.4 Internet Services

Relying on existing networks and dedicated connections, internet services are able to connect end users to the internet. Connectivity is provided through Internet Service Providers (ISPs) that offer packages for various use, internet backbone connectivity which links national and international connection points, and publicly available access points (Government of Ghana, 2004).

2.1.5 Roles of Government Institutions

This section classifies the roles that government institutions play in enacting Ghana's telecommunications policy.

2.1.5.1 Ministry of Communications and Digitalization

The ministry is the principal authority in shaping the components of telecommunications policy. In this position, they ensure robustness of the policy and update appropriately where necessary. The ministry also acts as a consultant in all regulatory proceedings led by the NCA (the primary industry regulator). The ministry as a representative of Ghana on international fronts such as ECOWAS in relation to the nation's telecommunication policies ensures the interests of the country are always protected. Finally, the ministry is also responsible for reporting and monitoring the status of the sector and tracking trends and concerns according to set goals (Government of Ghana, 2004).

The Ministry constitutes the below agencies and statutory bodies and through them, implements mandated operational and regulatory policies (Ministry of Communications, 2016):

1. Postal and Courier Services Regulatory Commission (PCSRC)
2. Ghana Meteorological Agency (GMet);
3. Ghana-India Kofi Annan Centre of Excellence in ICT (AITI-KACE):
4. National Information Technology Agency (NITA)
5. Data Protection Commission (DPC)

6. National Communications Authority (NCA)
7. Ghana Investment Fund for Electronic Communications (GIFEC)
8. Ghana Post Company Limited (GPCL)

2.1.5.2 National Communications Authority (NCA)

The NCA is the primary regulator of the telecommunications sector. It is also the instrument through which the National Telecommunications Policy is enacted. Its roles include being responsible for issuance of licenses, regulating competition among players, managing available spectrum frequencies, regulating tariffs, monitoring activities, performance and compliance with regulations of operators, upholding technical standards, overseeing quality of service and protecting the interests of consumers.

2.2 Ghana Cyber Security Policy

As emphasized earlier, society today is a more virtual world that relies on the internet for communication and business. Ghana's road to a more digitized economy which includes digitizing government services, building a biometric National Identity register, deploying a digital property addressing system, and mobile money interoperability among others, relies on the strength of Information and Communication Technologies (ICTs) (National Communications Authority, 2018). Increasing attacks on national infrastructure and government sites mandate protection of critical national information infrastructure to ensure national security in the wake of cyber wars. Activities of government can be brought to a halt if the National Information Technology Agency (NITA) infrastructure is attacked. Thus, policy was needed to manage the cyber security risks to government and private sector critical information infrastructure (Ministry of Communications, 2015).

The current cyber security policy and regulatory framework evolution has been as follows. In 2014 the Ministry of Communications inaugurated the Ghana Computer Emergency Response Team (CERT-GH) to coordinate national cyber security incidents. Approved by Cabinet in November 2016, Ghana adopted a National Cyber Security Policy and Strategy (NCSPS) (Media Foundation for West Africa, 2017, p. 14). This policy identifies specific initiatives to address cybercrime and cyber security issues as well as provides a strategy for implementation. Aside the NCSPS, specific legislations which address cyber security related issues have been passed by parliament: The Electronic Transactions Act – 2008 (Act 772), Data Protection Act – 2012 (Act 843), Economic & Organized Crime Act (EOCO) Act – 2010 (Act 804) and Anti-Money Laundering Act – 2008 (Act 749) (Media Foundation for West Africa, 2017). These Acts identify cyber security offences such as unauthorized access to protected information, stealing and electronic forgery, and child pornography. They also mandate organizations, like telecommunications companies, which fall within these remits to undertake regular vulnerability and systems checks to ensure robustness of IT systems that store, process and transmit particularly personal data. In 2020, Parliament passed the Cybersecurity Act – 2020 (Act 1038). This Act establishes a Cyber Security Authority, protects the critical information infrastructure of the country, regulates cybersecurity activities in the country, provides for the protection of children on the internet and promotes the development of cybersecurity and other related matters.

Through the Cybersecurity Act, 2020, the information and communications sector has been identified as Critical National Information Infrastructure (CNII). This category is "defined as those assets (real and virtual), systems and functions that are vital to the nation such that their incapacity or destruction would have devastating impact on national economic growth, national image, national defense and security and government capability to function" (Ministry of Communications, 2015).

The main institution dedicated to developing and effecting the national cyber security policy and strategy is the National Cyber Security Centre (NCSC). The NCSC is a national agency established in 2018 under the Ministry of Communications. “It is responsible for Ghana’s cybersecurity development including cybersecurity incidents response coordination within government and with the private sector. The NCSC is responsible for Awareness Creation & Capacity Building, Cybersecurity Incident Coordination & Response (CERT), Critical National Information Infrastructure Protection (CNIIP), Child Online Protection (COP) and International Cooperation, among others” (National Cyber Security Centre, 2019). The NCSC work closely with the National Cyber Security Technical Working Group (NCSTWG) in the implementation of cybersecurity initiatives across government and non-governmental sectors.

CHATPER 3
Research Method

3.0 Introduction

The primary objective of this study is to determine the extent to which and in what ways the cyber risk posture of Vodafone Ghana aligns with the Ghana National Telecommunications and Cyber Security policy framework. This chapter tackles the research methodology that supporting the study. It delves into the approaches, procedures and techniques employed in this study. Details of data collection, framework and analysis are also discussed. Finally, a discussion the critique associated with the selected method.

3.1 Approach to Study

This research employs qualitative method – one of the three major methods of the social sciences. This method was developed to allow scholars research social and cultural phenomena (Goundar, 2012). Qualitative research is defined as "any type of research that produces findings not arrived at by statistical procedures or other means of quantification" (Strauss & Corbin, 1998, pp. 10-11). Gay and Airasian (2000, p. 627) also define qualitative research as "the collection of extensive data on many variables over an extended period of time, in a naturalistic setting, in order to gain insights not possible using other types of research". However, these definitions largely depend on the essence of quantitative research which is described as "research that explains phenomena according to numerical data analyzed by means of mathematically based methods, especially statistics" (Yilmaz, 2013, p. 311). Thus to capture a definition that reflects its unique characteristics, Yilmaz (2013, p. 312) defines qualitative research as "an emergent, inductive, interpretive and naturalistic approach to the study of people, cases, phenomena, social situations and processes in their natural settings in order to reveal in descriptive terms the meanings that people attach to their experiences of the world". Berg (2007, p. 3) also captured that "quality refers to the what, how, when, and where of a

thing – its essence and ambience. Qualitative research thus refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things."

Qualitative research permits the researcher an insider view on the field of study. It plays an important role in uncovering possible relationships, causes, effects and dynamic processes (Goundar, 2012). Through descriptive and narrative style, the knowledge gained through qualitative investigations is more informative, richer and offers enhanced understandings compared to that of quantitative research (Tewksbury, 2009). Qualitative methods let the researcher record and understand people in their own terms, whereby depth and detail develop through direct quotation and meticulous description. Qualitative data is conducted through interviews, focus groups and participant's observation (Yunos & Ahmad, 2014). Despite these strengths, qualitative research is criticized for its problem of adequate validity or reliability due to its subjective nature. Thus, outcomes are limited to the context, conditions, events and interactions of the study. Another critique point is the lengthy time required for data collection, analysis and interpretation. There is also some extent of effect on the subjects of study posed by the researcher (Goundar, 2012).

This study aims to investigate cyber risk phenomenon focusing on the characteristics or features of cyber security which is exploratory in nature. Thus this qualitative research approach is relevant to the study because it is aimed at obtaining deep analysis of the case at hand rather than merely providing information from many units (Siaw, 2015).

3.2 Research Strategy

The identification of a research approach prescribes the strategies of enquiries associated with the research. Creswell (2003, p. 14) notes that key approaches to qualitative research include "ethnographies, case studies, grounded theory, phenomenological research, and narrative research". Research strategies are the manner in which the researcher plans to go about the research study (Siaw, 2015).

The strategy implemented is a case study. It can be used to describe a unit of analysis (e.g. a case study of a particular organization) or to describe a research method. Case study research is the most common qualitative method used in information systems (Goundar, 2012). Creswell (2003, p. 15) describes a case study as a kind of plan "in which the researcher explores in depth a program, an event, an activity, a process, or one or more individuals. The case(s) are bounded by time and activity…" Thus, a case study involves close observation and examination of the case or subject at hand.

The implementation of a case study as a research strategy drives and enables this research to enquire intensely into the extent to which and in what ways the risk posture of Vodafone Ghana aligns with the Ghana National Telecommunications and Cyber Security policy framework.

3.3 Data Collection Techniques

Data was collected using two main sources: primary and secondary sources. Primary sources included detailed individual interviews with respondents from relevant institutions to the study. Primary sources leverage the expert knowledge of relevant participants to study (Osuala, 2007). Secondary data included journals, articles, books, online sites and other relevant documents on cyber security.

To carry out this research, snowball sampling method was employed. This technique also called as 'chain referral' or 'networking' sampling where information gathering begins with one or a few people and generates other known colleagues who could be valuable participants to the study (Lopez & Whitehead, 2013). This chosen method facilitated collection of data in the niche of cyber security. A drawback of snowball sampling is that the researcher relies solely on referrals from initial contacts to generate other contributors. Thus, the participants are not a true reflection of the representation of the population of study (Lopez & Whitehead, 2013).

The research used detailed interview-based technique. Interviews are essential sources of information for case studies. Its structure is fluid and not rigid as it follows a guided conversational format rather than a structured query (Yin, 2003, p. 89). The interview method involves "presentation of oral-verbal stimuli and reply in terms of oral-verbal responses" (Kothari, 2004, p. 97). The interview will be semi-structured with a guide made of open-ended questions. Throughout the interview process, the guide will serve as a means to follow the study's line of inquiry. Open-ended questions allow less restrictive responses and some flexibility in how questions are asked, the order in which they are asked as well as choice to omit or include supplementary and follow-up questions. In this approach, respondents are free to determine the level and in-depthness of information to give. This sort of approach and flexibility, however, is critiqued for its results that are not comparable. The analysis of responses also tends to be more difficult and time consuming (Kothari, 2004). Interviews are also commonly prone to bias, poor recall, and poor or inaccurate articulation (Yin, 2003).

With the permission of the respondent, interviews will be recorded to facilitate accuracy of information recollection.

3.4 Data Analysis and Discussion

This section addresses the objectives of the study and responds to the research questions. It comprises a presentation and analyses of the views obtained from interviews conducted under the present study. It also employs secondary data from relevant literature.

3.4.1 Cyber risks in telecommunications companies

These can be categorized in two: internal and external risks or threats. Internal risks are mainly insider threat which results in data leakage and unauthorized access granted to parties not meant to have access. Insider threat is when employees purposely act in a malicious way (GSMA,

2019). Insiders who are privileged authorized users give information to unauthorized external users enabling them to have access to the network. These threats are by nature, very difficult to track as these authorized users have legitimate access to the system (Hau, 2003). They can misuse company's cyber resources to attack internally, access and disseminate critical information, change programming without authorization, steal data files for personal gain, and many more. This threat is monitored through User Access Management (UAM) also known as Logical Access Controls which tracks exactly when people access systems – who logs in and out and when. It can also control the type of accesses permitted to those with authorized access (Hau, 2003).

External risks include malware particularly ransomware, phishing, hacking, brute-force attack and credential stuffing. Malicious software, or malware for short (Konakalla & Veeranki, 2013, p. 274), are software that are built mainly to create an unauthorized entry point, or damage software or data without the knowledge of the person. There are many types such as spyware, viruses, worms, trojans, and key loggers. Ransomware, another type of malware particularly experienced by organizations like Vodafone, is a kind of malware that proliferates like a worm (Shah & Farik, 2017, p. 307) and restricts its users from having accessing to systems due to locked screens and files until the company pays the expected ransom (Deo & Farik, 2016, p. 219).

Phishing is a social engineering strategy that tries to tease out users' and organization's personal and private information (Konakalla & Veeranki, 2013, p. 273). Attackers attempt to find out information such as users login credentials and account information through deceptively posing as a trustworthy entity or individual via email (Deo & Farik, 2016, p. 218).

Hacking done by highly competent computer users can be people who are career criminals (Konakalla & Veeranki, 2013, p. 272). It is a top threat that can crack information system

securities (Deo & Farik, 2016, p. 219). Hackers analyze and exploit weak points in network systems. Attacks on systems are often done to steal information or money and sometimes to cause damage by inserting malware. Hacking done unbeknownst to targets is called unethical hacking (Deo & Farik, 2016, p. 219). They are constantly evolving in how they approach with attacks and introducing new vulnerabilities. Organizations are in a constant cycle of doing everything they can to get ahead of new hacking trends.

Brute- force attacks are a 'trial and error' method of guessing passwords (Dave, 2013, p. 75). Usual targets are websites or systems that require user authentication to go through. Attackers gather personal information such as user's names, children names, birthdate etc and continuously try several permutations and combinations of these until successful (Dave, 2013). It is an exhaustive and time-consuming search dependent on the strength and complexity of passwords (Forcepoint, 2021).

Credential stuffing attacks begin with cyber criminals purchasing previously used legitimate usernames and passwords off the black market. Targeting websites that require login authentication, they repeatedly attempt to "stuff" login fields with credentials to gain access to accounts held by corporate users or customers (F5 Netowrks, 2007, p. 2). This method relies on the chances of users reusing usernames and passwords. Successful attempts of this type of attack lead to fraudulent usage.

These identified risks are monitored and prevented through strong organizational policies. Implementing schedules for periodic password changes to login pages and enforcing the use of new, unique and strong credentials each time can reduce the chances of credential stuffing and brute-force attacks. Education through organizational awareness campaigns can raise the collective alertness of employees to recognize, identify and report phishing attempts and

obscure malicious software. Monitoring through UAM can help tackle cases of data leakage through unauthorized access.

3.4.1.1 Identification and monitoring of vulnerabilities

Identification of vulnerabilities occurs in collaboration with the parent company and other markets' organizations. There are specific teams responsible for incident response, defence, and intelligence. These teams span Africa, Europe and Asia. Recommended actions are disseminated to regions when vulnerabilities are identified. Periodic scanning is done internally by each market checking and ensuring the robustness of information systems and assets. Tools that perform end-point detection response also assist in flagging risks and vulnerabilities on employee devices, network servers and other assets. Further collaboration is done with network infrastructure teams to ensure fixing of vulnerabilities such as patch updates.

Other collaborators include the National Communications Authority cyber security team, Computer Emergency Response Team (CERT) for Ghana, and National Cyber Security Centre. These groups work together in intelligence gathering for the country, region, continent and beyond to ensure that preventive measures are put in place for identified vulnerabilities yet to be seen.

Monitoring of these vulnerabilities is done using diversified tools that handle specific areas - tools such as network intrusion detection system for network protections, firewalls for web domains, CISCO identity service engine for Local Area Network (LAN) protection preventing access by unauthorized users.

3.4.2 Risk management approach

This section deals with the governance, risk management strategy and flow of risk operations.

Governance is the structure of responsibilities practiced by those accountable for an organization (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 11). Good governance provides strategic direction, ensures achievement of organizational mission and business objectives, appropriate risk management and responsible resource use. A centralized approach to risk management is employed in this case study. A risk function or team has been established and tasked with organizational-wide approach to risk management. This team interfaces with all levels of organization from top management to security engineer level. Responsibilities of the risk team include: coordinating with operational teams and collating threats across the organization, serving as the key communication mouth-piece and oversight body of risk management activities, and ensuring effective decision making (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 13). Its place in the governance structure is to facilitate efficiency and maximize effectiveness. They liaise and communicate with all levels of organization from senior management to information system owners.

The general flow of risk management followed is a bottom-up approach. This strategy, spearheaded by the Business Risk team, is where risk is addressed from overhead operations that affect individual departments. The next level in this is 'tactical risk assessment' that entails the heads of departments and functional heads addressing risks pertaining to their respective functions. These risks are then collated and pushed to a 'priority risk level' where senior management has oversight of all risks to decide the top ten (10) risks for the organization.

Every organization has some system of assumptions they work with to determine how to go about aspects of risk management. These assumptions which are qualitative in nature, are collated through an organizational-wide scan to determine what is trending across business thus affecting individual departments and total business. Based on the organization's objectives, interviews are conducted with business teams to tease out possible risks, issues and hinderances

that could hinder the company's goals. Threat sources and events are determined through these in-depth interviews (horizon scanning) as well as trending industry risks. These are then discussed with subject matter experts to assess the vulnerabilities involved. Following these interviews, detailed action plans and trackers are developed to ensure oversight of mitigation actions to reduce identified risks. Thus, the team responsible for business risk acts as a second line of defense in collaboration with the teams that experience the risks. They monitor and provide assurance over agreed actions.

Risks are then categorized using a matrix framework that incorporates the level of impact and likelihood of occurrence. The categories on both scales are clearly defined and standardized as directed from the parent company across all branches in other countries. There are four (4) categories of likelihood rating – highly likely to occur, likely, possible and rare to occur. For the impact scale, the categories are very high, high, medium and low. Determining risk levels is a result of combination of these parameters. The bottom-up flow is used to communicate results of risk assessment to the organization.

A successful cyber-attack can cause significant harm to an organization. Potential impacts to organizations are financial, brand or reputational, operational, and legal and regulatory. Financial impacts arise from theft of corporate information, financial information, or money, or costs associated with losing contracts and the repair of impacted networks, systems and devices. When a business faces a cyber-attack, the trust and faith (essential elements of relationships) held among customers, investors, suppliers, and other third parties wanes thus are afraid to invest further in the organization (Yadav & Gour, 2014, p. 939). Customers are compelled to move onto other providers as they do not feel safe. The organization's reputation erodes and this further affects the bottom line. Operational losses include equipment loss in cases where malware destroys networking and information systems. Legal and regulatory impact can be in the form of fines and sanctions as laws such as the Data Protection Act, 2012

(Act 843) and Electronic Communications Act, 2008 (Act 775) require organizations to safeguard all personal data.

Typical risk constraints experienced in organizations revolve around availability and management of key stakeholders necessary for the outlined levels in the risk management flow. Due the nature of being second line of defense, the responsibility of follow ups on actions lay with them and "becomes tedious".

Another constraint is the organizational culture not reflecting a habit of risk management. NIST (2011, p. 28) defines culture as the unique values that guide the actions and activities of all members of the organization including top level management. This is not to say the organization is not aware, however it does not always reflect in day-to-day activities. This culture is more prevalent at the operational level – particularly heads of departments. Top level management has more awareness and response sensitivity to risk management activities. This sensitivity sets the tone and direction for risk tolerance and priorities.

Risk tolerance is "a combination of the cultural willingness to accept certain types of loss within organizations and the subjective risk-related actions of senior executives" (National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2011, p. 30). Factors such as the components of the organization's culture are considered when determining risk tolerance. These help reason decisions for risk trade-offs. The scale used to measure tolerance is pre-determined by the parent company. The scale comprises of three categories – not aligned, reasonably aligned and aligned. The first, not aligned, means there are major issues to a particular risk which need immediate attention. The second category, reasonably aligned to tolerance, means there are some ongoing mitigation steps in place to control the risk. The final category, aligned to tolerance, means there are very minor issues to be considered in the identified risks.

The next steps following risk assessment are to provide assurance and to submit the findings to the component bodies of the larger risk management framework of the organization. These oversight bodies, namely the risk council and the risk and audit committee. The risk council is made up of members of senior management, and the heads of internal audit and business risk teams. Their mandate is to review, assess and agree on all actions that may come up pertaining to identified risks. The risk and audit committee is a sub-committee of the organization's board and is independent in nature. Chaired by the head of internal audit, it comprises of the director of finance, two external board members, as well as some members of senior management. Issues discussed at these levels involve deciding the need for budget to address risks. They also exist to provide support on assurance and coordination of mitigation of risks.

Courses of action following the steps of risk assessment are determined uniquely on each presented case. Relevant stakeholders decide, bearing in mind the organization's interests and objectives, the best course of action – acceptance, avoidance, mitigation or transfer. Risks that threaten critical mission and organization objectives largely fall in the mitigation section of action. An example is the importance of cyber soundness in a company that holds large amounts of personal data which is critical to business operations. Thus, investing in robust systems to keep up with scanning, tracking, and logging of user accesses is critical. In cases of sharing or transferring risks, an insurance cover is employed in different fashions across business. In summary, the determinants are based on results of assessment of likelihood, impact and tolerance.

When it comes to implementation of the risk responses, following the structure and flow of the model of organizational risk management, all actions from identified risks are ensured to have specific timelines and a corresponding owner. Cyber risk monitoring is done with the oversight of the Chief Information Security Officer (CISO) and Chief Technology Officer (CTO).

Following the implementation of the actions, monitoring and effectiveness tracking is done by governance bodies who require periodic updates of the status of each risk. This is also bolstered by an automated system which notifies on pending and due actions.

These actions and activities of various stakeholders across levels of business, particularly top management being in the loop of cyber risk management show that there is not a total disconnect in the integration of cyber risk management and enterprise risk management.

3.4.3 Risk management innovations

In the spirit of advancements in technologies and ways of work, the subject of risk management is not excluded. Experts in enterprise risk look to more automated way of achieving the various steps in their risk management flow. Automated tools are more and more capable of being programmed to rank and categorize risks based on parameters outlined by the organization.

3.4.4 Cyber risk policy evolution

As outlined in earlier chapters, the national policy and framework consists of specific legislations which provide direction for handling of cyber security issues. These Acts have recently been supplemented by the Cybersecurity Act, 2020. Upon examination of these national provisions by expert respondents, their views are of the opinion that although the policies are sound, enforcement is lax and inadequate. A cited example is the nation's response to mobile money fraud which requires re-registration of SIM cards to ensure collection of proper authentic details. Systems necessary for this exercise are not ready for deployment yet. Cyber experts are of the view that regulatory bodies like the NCA and the Ministry of Communications need to do more.

Some expert respondents noted the wish to see cyber risk policy evolve to cyber insurance policy. Also referred to as cyber liability insurance coverage (CLIC), it is a "broad term for

insurance policies that address first and third party losses as a result of a computer-based attack or malfunction of a firm's information technology systems" (Romanosky, Ablon, Kuehn, & Jones, 2017, p. 2). The areas of coverage include network security liability, privacy liability, and communication and media liability and cyber extortion. Network security liability is coverage when third parties suffer losses due to intentional and unauthorized access to the insured's network (R & R Insurance). Privacy liability covers misappropriation or disclosure of personally identifiable information or a breach of laws associated with the control or use of personally identifiable information. Media liability covers defamation, libel or slander, or reputational harm (OECD, 2020). Extortion coverage takes care of situations where there are continuous breaches to network for the purpose of obtaining payment.

CHAPTER 4
Summary of Findings, Conclusion and Recommendations

4.0 Summary of findings

This study set out to explore the cyber risks encountered by telecommunications companies, their risk management approach in the framework of enterprise risk management, possible risk innovations as well as the cyber risk policy evolution of these telecom companies.

The study found that cyber risks experienced by telecom companies fall in two main categories: internal and external. Internal threats revolve around privileged users with legitimate access to systems using it for malicious gain. External threats are efforts by external parties in attempts to target systems, assets and employees to exploit vulnerabilities and weaken the IT structure of companies.

It was found that the organization's risk management approach followed the main tenets of the theoretical framework. There are structures in place to go through the steps of the risk management process: framing, assessing, responding and monitoring. These steps have been integrated into a multitiered framework that spans levels in the organization from the users and owners of the information systems to the heads of departments to senior management level. Component steps, functions and responsibilities of contributors to the process are clearly defined. Albeit drawback to do with stakeholder management and organizational culture which affect some aspects of the risk management process, the overall goal of tracking and keeping organizational risk in check is not lost and still achieved.

Risk assessment innovations are focused on the improvement of technology involved – automation of existing steps. Using purposely developed software and programs to enhance identification, categorization and monitoring of risks. Thus, ensuring effective action tracking and resolution.

Views on cyber policy effectiveness are of that although the provisions of relevant policies are adequate, enforcement is lax thus more attention is needed to ensure robust cyber security measures.

4.1 Conclusion

Telecommunications companies play a unique role in this Industry 4.0 society today. They handle large amounts of citizen's sensitive data in the critical networks they operate for fixed and mobile telephony. This makes them big targets for cyber-attacks. Attacks lead to sensitive data leakage which exposes affected individuals and organizations to risk (Agubor, Chukwudebe, & Nosiri, 2015, p. 128). To ensure risk coverage, organizations must implement strategies that are directly embedded in all levels of the business so that senior management, people and information systems are well versed in the common goal.

4.2 Recommendations

The telecommunications industry, relevant regulatory stakeholders and the government of Ghana can take several measures to equip itself to deal with cyber risks:

1. Industry collaboration – formation of governance structures that enable collaborative effort between telecommunications players in the country. This would encourage communication of unique threats affecting players and enable implementation of pre-emptive measures.

2. Public sector collaboration – synergizing government efforts with private sector efforts would boost the overall state of cyber security of the country.

3. Regional/international cooperation – to facilitate investigations and prosecution of cyber offenders as cyber targeting is borderless. Regional bodies such as ECOWAS should enhance directives on cybercrime for greater cooperation. Operationalization of the Africa Union

Convention on Cyber Security should also be prioritized to facilitate cross-border resilience among member states. Continued operationalization of the Budapest Convention and accession to future international treaties on cybercrime and cyber security would enhance preparedness.

4. Enforcement of existing legislations – ensuring that already developed policies deploy the necessary governance structures. Laws must keep up with and reflect technological advances.

5. Capacity building of law enforcement agencies – equipping relevant agencies and stakeholders with training and technology support to effectively assist in matters of cyber security at any level in the country.

6. Awareness campaign – to develop cyber security culture among citizens. Improving and increasing awareness of cyber risk among internet users should be done by all relevant stakeholders.

4.3 Further areas of research

Further research can be conducted in types of cyber fraud that plague the telecommunications industry: mobile money fraud and sim box fraud. Mobile money fraud, in the financial sector of operations includes "scams/impersonation, pin/password compromises, interception of mobile money tokens, attacks on merchants, unauthorized SIM swaps, system breaches and unauthorized access to customer/merchant's transactional data..." (Media Foundation for West Africa, 2017, p. 7).

Interconnect Bypass fraud, popularly known as SIM Box fraud in Ghana, is when perpetrators use internet-enabled devices known as SIM Boxes to convert international calls and make them appear as local ones (Nyarko-Boateng, 2018). This results in bypassing the regular international interconnect rates set by operators to pay a considerably lower local termination

rate. This results in revenue loss, tax discrepancies and poor customer experience (Kouam, Viana, & Tchana, 2021).

In conclusion, there is room for more impactful research in cyber security and telecommunications

BIBLIOGRAPHY

African Union. (n.d.). Retrieved October 3, 2020, from CCDCOE: https://ccdcoe.org/organisations/au/

African Union. (2014, June 30). *The 23rd ordinary session of the African Union ends in Malabo*. Retrieved September 29, 2020, from African Union: https://au.int/en/newsevents/29258/23rd-ordinary-session-african-union-ends-malabo

African Union. (2020, June 18). *African Union convention on cyber security and data protection.* Retrieved October 2, 2020, from African Union: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

African Union adopts framework on cyber security and data protection. (2014, August 22). Retrieved September 29, 2020, from Access Now: https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/

Agubor, C. K., Chukwudebe, G. A., & Nosiri, O. C. (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. *International conferencce on cyberspace governance*, (pp. 124-128). Abuja. Retrieved January 29, 2020, from https://www.researchgate.net/publication/301649544_Security_Challenges_to_Telecommunication_Networks_An_Overview_of_Threats_and_Preventive_Strategies

Agubor, C. K., Chukwudebe, G. A., & Nosiri, O. C. (2015). Security challenges to telecommunication networks: An overview of threats and preventive strategies. *2015 International Conference on Cyberspace Governance - CYBERABUJA2015*, (pp. 124-129). Owerri.

Agyekum, F. (2010, March). No apologies for Ghana Telecom-Vodafone Deal, says Kufuor. *New African*, pp. 72-75.

Ajao, O. D. (2009, April 16). *Ghana Telecom and Onetouch are now Vodafone Ghana*. Retrieved from Tech Dot Africa: https://tech.africa/ghana-telecom-and-onetouch-are-now-vodafone-ghana/

Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 62-77.

Barton, T. L., Shenkir, W. G., & Walker, P. L. (2002). *Making enterprise risk management pay off: How leading companies implement risk management.* New Jersey: Financial Times/Prentice Hall PTR.

Baylon, C., & Antwi-Boasiako, A. (2016, November 14). *Increasing internet connectivity while combatting cybercrime: Ghana as a case study.* Retrieved September 30, 2020, from Centre for International Governance Innovation: https://www.cigionline.org/sites/default/files/documents/GCIG%20no.44_0.pdf

BBC News. (2019, May 21). *Ren Zhengfei says US government 'underestimates' Huawei*. Retrieved October 3, 2020, from BBC News: https://www.bbc.com/news/business-48345742

Behrent, M. C. (2013). Foucault and technology. *History and Technology*, 54–104.

Berg, B. (2007). *Qualitative research methods for the social sciences 6th edition.* Boston: Pearson Education.

Biener, C., Eling, M., & Wirfs, J. H. (2015). Insurability of cyber risk: An empirical analysis. *The Geneva Papers on Risk and Insurance- Issues and Practice*, 131-158. Retrieved from https://www.alexandria.unisg.ch/238242/1/Insurability%20of%20Cyber%20Risk%20An%20Empirical%20Analysis.pdf

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *New Seurity Paradigms Workshop*, (pp. 97-104). Retrieved July 3, 2021, from https://www.nspw.org/papers/2001/nspw2001-blakley.pdf

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, 266.

Bulletproof. (2019). *Bulletproof annual cyber security report 2019.* Retrieved October 4, 2020, from https://www.bulletproof.co.uk/industry-reports/2019.pdf

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 43-2.

Casualty Actuarial Society. (2003). Overview of enterprise risk management. Retrieved from https://www.casact.org/area/erm/overview.pdf

Cavelty, M. D., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 1-28. doi:10.1080/13523260.2019.1678855

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, 70-7.

CIMA. (2008). Introduction to managing risk. *Topic Gateway series*. Retrieved July 22, 2019, from http://www.cimaglobal.com/Documents/ImportedDocuments/cid_tg_intro_to_managing_risk.apr07.pdf

Clement, J. (2020, July 24). *Global digital population as of July 2020*. Retrieved September 29, 2020, from Statista: https://www.statista.com/statistics/617136/digital-population-worldwide/

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environmental Systems and Decisions, 33*, 469-470. doi:10.1007/s10669-013-9484-z

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004, September). Enterprise risk management — integrated framework: Executive summary. Retrieved from https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Council of Europe. (2018, December 3). *Ghana accedes to the Budapest convention on cybercrime*. Retrieved October 8, 2020, from Council of Europe: https://www.coe.int/en/web/cybercrime/-/ghana-accedes-to-the-budapest-convention-on-cybercrime

Council of Europe. (n.d.). *Details of Treaty No.185*. Retrieved October 9, 2020, from Council of europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Creswell, J. W. (2003). *Research design: Qualitative, quantitative and mixed method approaches (2nd ed).* Thousand Oaks: Sage.

(2017). *Cyber security in Ghana: Key issues and challenges.* Accra: Media Foundation for West Africa (MFWA). Retrieved February 1, 2020, from https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf

Cyber security trends and government responses in Africa. (n.d.). Retrieved October 3, 2020, from Broadcom: https://www.broadcom.com/info/symantec/cyber-security-trends-africa

Daily Graphic. (2019, December 11). *SIM box fraud: State loses GH¢3m monthly*. Retrieved from GhanaWeb: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/SIM-box-fraud-State-loses-GH-3m-monthly-811882

Darko, S. (2015, May 9). *Inside the world of Ghana's internet fraudsters*. Retrieved September 30, 2020, from BBC News: https://www.bbc.com/news/world-africa-32583161

Daskal, J., & Kennedy-Mayo, D. (2020, July 2). *Budapest convention: What is it and how is it being updated?* Retrieved October 8, 2020, from Cross-Border Data Forum: https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/

Dave, K. T. (2013, June). Brute-force attack "seeking but distressing". *International Journal of Innovations in Engineering and Technology, 2*(3), 75-78.

DDoS attack statistics: A look at the most recent and largest DDoS attacks. (2020, March 6). Retrieved October 4, 2020, from InfoSec Insights: https://sectigostore.com/blog/ddos-attack-statistics-a-look-at-the-most-recent-and-largest-ddos-attacks/

Deloitte. (2017). *Industry 4.0 and cybersecurity: Managing risk in an age of connected production.* Connecticut: Deloitte Development LLC.

Deloitte. (2019). *Governance and enterprise risk management: Managing cyber risk in a digital age.* North Carolina: Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Deo, S., & Farik, M. (2016, December). Information security - recent attacks in Fiji. *International Journal of Scientific & Technology Research, 5*(12), 218-220.

Dickinson, G. (2001). Enterprise risk management: Its origins and conceptual foundation. *The Geneva Papers on Risk and Insurance, 26*(3), 360-366.

Dickinson, G. (2001). Enterprise risk management: its origins and conceptual foundations. . *The Geneva Papers on Risk and Insurance-Issues and Practice*, 360-366.

Dunn Cavelty, M., & Suter, M. (2009). Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, 1-9. doi:https://doi.org/10.1016/j.ijcip.2009.08.006

Eling, M., McShane, M., & Nyugen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 93-125. doi:10.1111/rmir.12169

Ellott, M., & Kpodo, K. (2008, July 3). *Vodafone acquires 70 percent stake in Ghana Telecom*. Retrieved August 21, 2020, from Reuters: https://www.reuters.com/article/us-vodafone-ghana/vodafone-acquires-70-pct-stake-in-ghana-telecom-idUSL0358252520080703

Ennin, D., & Mensah, R. O. (2019). Cybercrime in Ghana and the Reaction of the Law. *Journal of Law, Policy and Globalization*, Vol 84, pp 36-45.

Ervural, B. C., & Ervural, B. (2018). Overview of cyber security in the industry 4.0 era. In A. Ustundag, & E. Cevikcan, *Industry 4.0: Managing the digital transformation* (pp. 267-284). Switzerland: Springer International Publishing. Retrieved from https://www.researchgate.net/publication/319861803_Overview_of_Cyber_Security_in_the_Industry_40_Era

Etzioni, A. (2014). The private sector: A reluctant partner in cybersecurity. *Georgetown Journal of International Affairs*, 69-78.

F5 Netowrks. (2007). Credential stuffing: A security epidemic. F5 Networks, Inc. Retrieved June 13, 2021, from https://networksunlimited.africa/images/PDFs/F5/eBook_Credential%20Stuffing_EN.pdf

Forcepoint. (2021). *What is a brute force attack?* Retrieved June 14, 2021, from Forcepoint: https://www.forcepoint.com/cyber-edu/brute-force-attack

Foster, W., Goodman, S., Osiakwan, E., & Bernstein, A. (2004). Global diffusion of the internet IV: The internet in Ghana. *Communications of the Association for Information Systems*, 1-47. doi:10.17705/1CAIS.01338

Fraser, J. R., Schoening-Thiessen, K., & Simkins, B. J. (2011). Who reads what most often?: A survey of enterprise risk management literature read by risk executives. In J. Fraser, & B. J. Simkins, *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives* (pp. 390-402). New Jersey: John Wiley & Sons Inc.

Freedman, L. (1998). International security: Changing targets. *Foreign Policy*, 110, 48—63.

Frost, & Sullivan. (2017). *Cyber security in the era of industrial IoT.* Frost & Sullivan White. Retrieved from https://ww2cdn.frost.com/wp-content/uploads/2017/02/FS_WP_Cyber-Security-in-the-Era-of-Industrial-IoT_200217.pdf

Gay, L. R., & Airasian, P. (2000). *Educational research: competencies for analysis and application* (6th ed.). Upper Saddle River: Prentice Hall.

Ghana Post. (2020). *About Ghana Post*. Retrieved August 22, 2020, from Ghana Post: https://ghanapost.com.gh/ghana-post/

Ghananewsagency.org. (2019, May 3). *Ghana lost US$105 million in 2018 through cybercrime*. Retrieved January 22, 2020, from GhanaWeb: https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Ghana-lost-US-105-million-in-2018-through-cybercrime-743261

Giles, K., & Hagstead, W. (2013). Divided by a common language: Cyber definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, & M. Maybaum (Ed.), *5th International Conference on Cyber Conflict* (pp. 1-17). Tallinn: CCD COE Publications.

Goldsmith, J. (2011, March 9). Cybersecurity treaties: A skeptical view. `. Retrieved August 5, 2020, from https://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf

Goundar, S. (2012, March). Research methodology and research method. Retrieved November 4, 2020, from https://www.researchgate.net/publication/333015026_Chapter_3_-_Research_Methodology_and_Research_Method

Government of Ghana. (2004). National Telecommunications Policy. Republic of Ghana: Government of Ghana.

GSMA. (2019). *Mobile telecommunications security threat landscape.* London: GSMA. Retrieved from https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf

Haggarty, L., Shirley, M. M., & Wallsten, S. (2002, November). Telecommunication Reform in Ghana. *SSRN Electronic Journal*. doi:10.2139/ssrn.373960

Harris , S. (2002). *CISSP certification exam guide.* McGraw-Hill/Osbourne.

Hau, D. (2003, July 11). Unauthorized access - threats, risk and control. SANS Institute. Retrieved May 21, 2021, from https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264

Hoijtink, M., & Leese, M. (2019). *Technology and agency in international relations.* London: Routledge.

Holt, G. A. (1996). *Closed Form Value at Risk. Contingency Analysis.* Retrieved from http://www.contingencyanalysis.com/frame/framevar.htm.

Howard, J. D., & Longstaff, T. A. (1998). *A common language for computer security incidents.* Albuquerque, Livemore: Sandia National Laboratories. Retrieved from https://www.researchgate.net/publication/2428384_A_Common_Language_for_Computer_Security_Incidents

Imperva. (n.d.). *Phishing attacks*. Retrieved October 4, 2020, from Imperva: https://www.imperva.com/learn/application-security/phishing-attack-scam/

Infinit-O. (2018, April). *The 5 pillars of information security and how to manage them*. Retrieved from Infinit-O: https://resourcecenter.infinit-o.com/blog/the-5-pillars-of-information-security-and-how-to-manage-them/

Insua, D. R., Couce-Vieira, A., Runio, J. A., Pieters, W., Labunets, K., & Rasines, D. (2019). An adversarial risk analysis framework for cybersecurity. *Risk Analysis*, 16-36. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1111/risa.13331

International Telecommunications Union. (2008). *ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cyber security.* Geneva: ITU. Retrieved from https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1205-200804-I!!PDF-E&type=items

International Telecommunications Union. (2019). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU Publications. Retrieved September 30, 2020, from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunications Union. (2019). *Measuring digital development: Facts and figures 2019.* Retrieved January 22, 2020, from International Telecommunications Union: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf

ISO/IEC. (2016). *ISO/IEC 27000:2016(en) information technology — security techniques — information security management systems — overview and vocabulary*. Retrieved from ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

ITU. (n.d.). *ECOWAS*. Retrieved September 24, 2020, from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/gpECOWAS.aspx

Junp, P. W. (2011). A critical analysis on the concept of cyber cecurity. *Yonsei Journal of Medical and Science Technology Law*, 1-25.

Kerstin, D., Simone, O., Nicole, Z., & Lehner, O. M. (2014, November). Challenges in Implementing Enterprise Risk Management. *ACRN Journal of Finance and Risk Perspectives, 3*(3), 1-14. Retrieved May 18, 2022, from http://www.acrn-journals.eu/resources/jfrp201403a.pdf

Keyser, M. (2003). The Council of Europe convention on cyber crime. *Journal of Transnational Law & Policy*, 287–326.

Kloman, H. F. (1976, July). The risk management revolution.

Konakalla, A., & Veeranki, B. (2013, November). Evolution of security attacks and attacks and security technology. *International Journal of Computer Science and Mobile Computing, 2*(11), 270-276.

Kothari, C. R. (2004). *Research methodology: Methods & techniques.* New Delhi: New Age International (P) Ltd Publishers.

Kouam, A., Viana, A. C., & Tchana, A. (2021). *SIMBox bypass frauds in cellular networks: a survey.* INRIA. Retrieved June 15, 2021, from https://hal.inria.fr/hal-03105845/file/The_SIMbox_fraud_survey.pdf

Kshetri, N. (2014). Cybersecurity and international relations: The U.S. engagement with China and Russia. *FLACSO-ISA 2014*, (pp. 1-38). Buenos Aires.

Kshetri, N. (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 77-81.

Kure, H. I., Islam, S., & Razzaque, M. A. (2018, May 30). An integrated cyber security risk management approach for a cyber-physical system. *Applied Sciences, 8*(6), 1-29. Retrieved July 1, 2021, from https://www.mdpi.com/2076-3417/8/6/898/htm

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate goverance, social responsibility and data breaches. *Financial Review, 53*(2), 413-455. Retrieved from https://onlinelibrary.wiley.com/doi/abs/10.1111/fire.12160

Liebi, M. (2016, May 25). *Industry 4.0 and the Impact on Cybersecurity*. Retrieved from United Security Providers: https://www.united-security-providers.com/blog/industry-4-0-and-the-impact-on-cybersecurity/

Lipson, C. (1991). Why are some international agreements informal? *International Organization*, 495-538.

Löfgren, K. (2013, May 19). Qualitative analysis of interview data: A step-by-step guide for coding/indexing. Retrieved November 28, 2020, from https://www.youtube.com/watch?v=DRL4PF2u9XA

Lopez, V., & Whitehead, D. (2013). Sampling data and data collection in qualitative research. In D. Whitehead, G. LoBiondo-Wood, & J. Haber, *Nursing and midwifery research: Methods and appraisal for evidence based practice* (4th ed., pp. 123-140). Elsevier - Mosby. Retrieved November 26, 2020, from

https://www.researchgate.net/publication/255950308_Sampling_data_and_data_collection_in_qualitative_research

Mathe, A. (2019, July 10). *The misunderstood world of cybersecurity in Africa*. Retrieved September 30, 2020, from Policy center for the New South: https://www.policycenter.ma/opinion/misunderstood-world-cybersecurity-africa#.X3VPz2j7Q2x

Media Foundation for West Africa. (2017, June). Cyber security in Ghana: Key issues and challenges. Media Foundation for West Africa. Retrieved June 10, 2021, from https://www.mfwa.org/wp-content/uploads/2017/09/cyber-security-Report.pdf

Ministry of Communications. (2015, July 23). Ghana national cyber security policy & strategy. Ghana. Retrieved October 6, 2020, from https://www.academia.edu/37141183/NATIONAL_CYBER_SECURITY_POLICY_AND_STRATEGY_REPUBLIC_OF_GHANA

Ministry of Communications. (2016). *About us*. Retrieved from Ministry of Communications: https://www.moc.gov.gh/about

Ministry of Communications. (2017). *National Cyber Security Week Report.* Accra: Ministry of Communications.

Murynets, I., Zabarankin, M., Jover, R. P., & Panagia, A. (2014). Analysis and detection of SIMbox fraud in mobility networks. *IEEE Conference on Computer Communications.*

National Communications Authority. (2018, December). Our contributions in 2018 towards Ghana's digital agenda. Retrieved October 9, 2020, from https://www.nca.org.gh/assets/Uploads/Key-NCA-Projects-2018.pdf

National Communications Authority. (2019, November). *Telecoms data subscriptions*. Retrieved from National Communications Authority: https://www.nca.org.gh/industry-data-2/market-share-statistics-2/telecom-data-subs/

National Communications Authority. (2020). Mobile data subscriptions from January to March 2020. Ghana. Retrieved September 30, 2020, from https://www.nca.org.gh/assets/COMMUNICATIONS-INDUSTRY-STATISTICS-MD-Q1.pdf

National Cyber Security Centre. (2019). *About us who we are*. Retrieved October 2, 2020, from National Cyber Security Centre: https://cybersecurity.gov.gh/about

National Cyber Security Centre. (2019). *Who we are?* Retrieved from National Cyber Security Centre: https://cybersecurity.gov.gh/about

National Institute of Standards and Technology (NIST), U.S. Department of Commerce. (2011, March). Managing information security risk: Organization, mission and information system view. *Special Publication 800-39*.

NetScout. (2019). *Netscout threat intelligence report.* NetScout. Retrieved October 4, 2020, from https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf

Nibusinessinfo.co.uk. (n.d.). *Cyber security for business: Impact of cyber attack on your business*. Retrieved June 15, 2021, from Nibusinessinfo.co.uk: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

Nyarko-Boateng, O. (2018, January 28). *SIM box fraud in Ghana: The control mechanisms*. Retrieved June 16, 2021, from Institute of ICT Professionals Ghana: https://iipgh.org/sim-box-fraud-ghana-control-mechanisms/

Nyarko-Yirenkyi, A. (2020, March 3). *Ghana loses $9.8m to cybercrime, other criminal activities in 2019*. Retrieved September 30, 2020, from Ghananian Times: https://www.ghanaiantimes.com.gh/ghana-loses-9-8m-to-cybercrime-other-criminal-activities-in-2019/

Nye, J. S. (2010). *Cyber Power.* Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

OECD. (2020). Encouraging clarity in cyber insurance coverage: The role of public policy and regulation. Retrieved June 15, 2021, from https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

Osei-Owusu, A. (2017). Policy foundation of the Ghana telecom industry. *Journal of NBICT*, 45–64.

Osuala, E. (2007). *Introduction to research methodology.* Nigeria: Africana- First Publishers.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Manufacturing Engineering Society International Conference 2017, MESIC 2017, 28-30 June* (pp. 1253-1260). Spain: Elsevier.

R & R Insurance. (n.d.). Understanding Cyber Liability Insurance. Retrieved June 18, 2021, from https://cdn2.hubspot.net/hubfs/136908/docs/e-books/RRI-Understanding-Cyber-Liability-Insurance.pdf

Raggad, B. G. (2010). *Information security management: Concepts and practice.* New York: CRC Press.

Ramseyer, J. M. (1991). Legal rules in repeated deals: Banking in the shadow of defection in Japan. *Journal of Legal Studies*, 91-117.

Rattray, G. (2001). *Strategic warfare in cyberspace.* Cambridge: The MIT Press.

Reuters. (2019, February 21). *U.S. won't partner with countries that use Huawei systems: Pompeo*. Retrieved October 3, 2020, from Reuters: https://www.reuters.com/article/us-huawei-tech-usa-pompeo-idUSKCN1QA1O6

Rojko, A. (2017). Industry 4.0 concept: Background and overview. *International Journal of Interactive Mobile Technologies*, 77-90.

Roller, M. R., & Lavrakas, P. J. (2015). *Applied qualitative research design: A total quality framework approach.* New York: The Guilford Press.

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2017). Content analysis of cyber insurance policies: How do carriers price cyber risk? Retrieved June 18, 2021, from https://www.ftc.gov/system/files/documents/public_comments/2017/10/00012-141437.pdf

Schreier, M. (2012). *Qualitative Content Analysis in Practice.* London: Sage.

Sentuna, A., Alsadoon, A., Prasad, P. W., Saadeh, M., & Alsadoon, O. H. (2020). A novel enhanced bayes posterior probability (ENBPP) using machine learning: Cyber threat analysis. *Neural Processing Letters*, 1-33.

Seunghwan, Y., Birch, A. S., & Bengtsson, H. I. (2016). The Role of State Actors in Cybersecurity: Can State Actors Find Their Role in Cyberspace? In E. de Silva, *National Security and Counterintelligence in the Era of Cyber Espionage* (pp. 217-246). IGI Global.

Shah, N., & Farik, M. (2017). Ransomware - threats, vulnerabilities And recommendations. *International Journal of Scientific & Technology Research, 6*(6), 307-309.

Shetty, S., McSchane, M., Zhang, L., Kesan, J. P., Kamhoua, C. A., Kwiat, K., & Njilla, L. L. (2018). Reducing informational disadvantages to improve cyber risk management. *The Geneva Papers on Risk and Insurance - Issues and Practice, 43*(2), 224-238.

Siaw, E. K. (2015, July). Change and continuity in Ghana's foreign policy: focus on economic diplomacy and good neighbourliness under Rawlings and Kufuor. Accra, Ghana.

Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, 1-37.

Sobel, P. J., & Reding, K. F. (2004). Aligning corporate governance with enterprise risk management. *Management Accounting Quarterly, 5*(2), 29-37.

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020, October). Integrating cybersecurity and enterprise risk management (ERM). *NISTIR 8286*. United States: National Institute of Standards and Technology. Retrieved July 3, 2021, from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf

Strauss, A. L., & Corbin, J. (1998). *Basics of qualitative research: techniques and procedures for developing grounded theory.* Thousand Oaks: Sage.

Telegeography. (n.d.). *SAT-3/WASC*. Retrieved August 23, 2020, from Submarine cable networks: https://www.submarinenetworks.com/en/systems/euro-africa/sat-3#:~:text=The%20South%20Atlantic%20Telecommunications%20cable,ready%20for%20service%20in%202001.&text=The%20SAT%2D3%20is%20also,called%20SAT%2D3%2FWASC.

Testrig. (n.d.). *Relationship between cyber security and risk management*. Retrieved from Testrig: https://www.testrigtechnologies.com/relationship-between-cyber-security-and-risk-management/

Tewksbury, R. (2009). Qualitative versus quantitative methods: Understanding why qualitative methods are superior for criminology and criminal justice. *Journal of Theoretical and Philosophical Criminology*, 38-58.

The Economist. (2010, July 1). *War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?* Retrieved August 2, 2020, from The Economist: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

Tsakanyan, V. T. (2017). The role of cybersecurity in world politics. *Vestnik RUDN. International Relations*, 339-348.

Turner, T. L., Balmer, D. F., & Coverdale , J. H. (2013). Methodologies and study designs relevant to medical education research. *International Review of Psychiatry*, 25(3) pp.301-310.

Valentine, E. L. (2016, October 14). Enterprise technology governance: New information and technology core competencies for boards of directors. *Doctoral Dissertation*. Queensland University of Technology. Retrieved July 5, 2021, from https://www.researchgate.net/publication/309132797_Enterprise_technology_governance_New_information_and_technology_core_competencies_for_boards_of_directors

Vaswani, K. (2019, March 6). *Huawei: The story of a controversial company*. Retrieved October 3, 2020, from BBC News: https://www.bbc.co.uk/news/resources/idt-sh/Huawei

Vodafone. (n.d.). Retrieved August 20, 2020, from crunchbase: https://www.crunchbase.com/organization/vodafone

Vodafone Ghana. (2020). *Our Brand*. Retrieved August 21, 2020, from Vodafone Ghana: https://vodafone.com.gh/explore-vodafone/about-us/our-brand/

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 97-102.

Wall, D. (2007). *Cybercrome.* Cambridge: Polity.

Warner, J. (2011). Understanding cyber-crime in Ghana: A view from below. *International Journal of Cyber Criminology*, 736-749. Retrieved from https://www.cybercrimejournal.com/warner2011ijcc.pdf

Weill, P., & Ross, J. W. (2004). *IT governance: how top performers manage IT decision rights for superior results.* Harvard Business School Press.

Whalen, J., Lerman, R., & Nakashima, E. (2020, September 18). *U.S. bans WeChat, TikTok as China becomes major focus of election*. Retrieved October 4, 2020, from Washington Post: https://www.washingtonpost.com/technology/2020/09/18/tiktok-wechat-ban-trump/

Yadav, H., & Gour, S. (2014). Cyber attacks: An impact on economy to an organization. *International Journal of Information & Computation Technology, 4*(9), 937-940.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*, 311-325. Retrieved from https://qualethics101.files.wordpress.com/2016/10/yilmaz-2013.pdf

Yin, R. K. (2003). *Case study research: Design and methods third edition.* Thousand Oaks: Sage Publications Inc. Retrieved from https://iwansuharyanto.files.wordpress.com/2013/04/robert_k-_yin_case_study_research_design_and_mebookfi-org.pdf

Yunos, Z., & Ahmad, R. (2014). The application of qualitative method in developing a cyber terrorism framework. *International Conference on Economics, Management and Development*, (pp. 133-137). Retrieved from http://universitypress.org.uk/library/2014/interlaken/bypaper/ECON/ECON-18.pdf

APPENDIX
INTERVIEW GUIDE

INTRODUCTION

This research's aim is to investigate the extent to which and in what ways the risk posture of Vodafone Ghana aligns with the Ghana National Telecommunications and Cyber Security policy framework. The interview was structured according to previously mentioned research questions.

A. 1. What are the cyber risks encountered by telecommunication companies in Ghana?

B. What is the risk management approach of these telecommunication companies?

2. What general flow of risk management is followed in your organization?
3. How is the risk management strategy applied across levels in the organization?
4. How do you identify assumptions that affect how risk is assessed, responded to, and monitored within the organization? What factors influence these assumptions?
5. How does your organization identify and characterize threat sources and events?
6. How do you identify and characterize cyber vulnerabilities? Are these vulnerabilities communicated across the organization? If yes, how?
7. What approach is used to determine likelihood of threat occurrences?
8. What are the types of impact/consequences that could be experienced? How do you assess impacts/consequences to operations, assets, external partners and the nation?
9. What are typical constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization?
10. How is risk tolerance determined in your organization? What techniques are used to define this tolerance?
11. How do you carry out risk assessment? Is it done at all levels of the organization? How is it conducted across all levels? Are there organizationally defined and applied processes?
12. What is the outcome from risk assessments? What are the next steps?
13. How are courses of action determined? i.e. deciding to accept, avoid, mitigate, share or transfer risk. What factors lead to determination of (each of) these actions?
14. How are risk responses implemented? What factors play in this implementation?
15. How does your organization monitor risk? What tools, techniques and procedures are used? Automated or manual monitoring? How frequent are these monitoring activities? How do you check effectiveness of these implemented actions?

C. 16. What are the possible risk assessment innovations?

D. What is the cyber risk posture policy evolution of these telecommunication companies?

17. Where do you see cyber risk policy evolving to next?
18. Is the current national policy adequate? If yes, why? If no, why?
19. In your opinion, what is lacking in the current national cyber policy with respect to operations of telecommunication companies?