University of Nairobi

Faculty of Science and Technology

Department of Computing and Informatics

A CYBERSECURITY ASSESSMENT OF THE REMOTE WORKING ENVIRONMENT DURING COVID-19. A CASE STUDY OF FINANCIAL REGULATORS IN KENYA

Douglas Mwaniki Ngere

P54/38758/2020

Supervisor: Dr. Samuel Ruhiu

A Research Project submitted in Partial Fulfilment of the requirements for the award of Master of Science in Information Technology Management, Faculty of Science and Technology, University of Nairobi.

DECLARATION

I declare that this research proposal is my original work, and it has not been presented in any other University or Institution of Learning for the award of a degree.

Signature: Date: 16th June 2022

Name: **Douglas Mwaniki Ngere**

Reg. No: **P54/38758/2020**

This research project has been submitted for examination for the fulfillment for the award of Master of Science in Information Technology Management with my approval as the University Supervisor.

Signature: **Date: 21/06/2022**

Name: DR. Samuel Ruhiu

Faculty of Science and Technology

ACKNOWLEDGEMENT

This thesis has been developed under the valuable guidance of my supervisor, Dr. Samuel Ruhiu. I acknowledge my fellow comrades for their insights and ideas for they were of great help. My appreciation to my family for their invaluable support and to God who makes all things possible.

ABSTRACT

The Covid-19 pandemic abruptly transformed the way businesses and organizations operate, with governments around the world implementing measures to protect people in order to slow the spread of the virus. This included strict lockdowns and social distancing measures that caused entire workforces to adopt remote working. Organizations therefore had to devise ways support the new arrangement with no time to prepare their ICTs, put in place necessary security mechanisms and develop appropriate policies to guide accessibility of resources from remote locations. As a result of this sudden and unplanned shift to work from home and shift operations online, malicious cyberspace activities and emergent threats proliferated to exploit vulnerabilities in ICT's. Little research exists on how pandemics such as Covid-19 present opportunities for cybercriminals to perpetrate their activities. The study aimed to investigate how different factors such as cybersecurity preparedness, cybersecurity management procedures and cybersecurity threats influenced remote. Literature revealed that there was a significant increase in cyberthreat activities such as malware, ransomware, and phishing attacks which targeted unprotected and unsuspecting victims during remote working. This research study adopted the quantitative research approach where data was collected using self-administered questionnaires where descriptive statistics and regression analysis was conducted. Based on the regression model, the findings demonstrated that where cybersecurity preparedness measures and cybersecurity management procedures were adopted, they had a significant positive effect in aiding the financial regulatory institutions to achieve secure remote working. However, with the proliferation of cybersecurity threats, and where these were encountered in some form, this impacted negatively to the remote working environment which became vulnerable. In the same way, adoption of cybersecurity frameworks led to a more secure remote working environment. This research proposed and validated a model that explains how these different aspects interplay to affect cybersecurity of the remote working environment. However, development of a model that can be used to mitigate cybersecurity risks for secure remote working is recommended during the remote working period. This study is expected to generate interest among ICT stakeholders in both public and private organizations about the emergent cybersecurity to securing their information assets and the remote worker during the Covid-19 pandemic and beyond.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

Figures

Tables

ABBREVIATIONS/ACROYNMS

APT	Advanced Persistent Threat
BYOD	Bring Your Own Device
CMA	Capital Markets Authority
Covid-19	Coronavirus Disease 2019
DDOS	Distributed Denial of Service Attacks
FBI	Federal Bureau of Investigations
GDPR	The General Data Protection Regulation
ICTs	Information, Communication and Technology
ITIL	Information Technology Infrastructure Library
IRA	Insurance Regulatory Authority
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
RBA	Retirements Benefits Authority
RDP	Remote Desktop Protocol
SaaS	Software as a Service
SIM	Subscriber Identity Module
SOC	Security Operations Centre
SPSS	Statistical Package for Social Sciences
VPNs	Virtual Private Network (s)
WFH	Work-from-Home
STSD	Socio-Technical Systems Design
ILO	International Labour Organization
SCT	Social Cognitive Theory
SLT	Social Learning Theory

1.0 CHAPTER ONE

Background of the Study

Following the outbreak of Covid-19 at the end of 2019 and early 2020 around the globe, businesses, governments, corporations, and organizations were compelled to innovate and change the way they conduct their work(Savić, 2020). The Covid-19 pandemic transformed the way businesses and organizations operate with governments around the world implementing regulations to protect people in order to slow the spread of the virus, which included strict lockdowns and social distancing measures that have caused entire workforces to adopt remote working (Malecki, 2020).

However, prior to the Covid-19 pandemic, remote working was not a widely adopted concept in organizations (Kossek and Lautsch, 2018). It was common to find organizations that had no remote employees or the percentage of the work force that was fully remote was comparatively small (Ozimek, 2020). Regardless, organizations, business operations and services needed to continue effectively and uninterrupted with the employment of ICTs in novel ways to meet this challenge; with the migration to online services for remote working through technologies such as cloud computing, VPNs, virtual dash-boards, and the Internet facilitating this digital transformation (Weil and Murugesan, 2020). Today's practices have changed and working from home has become acceptable for organizations and employees who want to have a flexible and self-controlled way of working (Gallardo, & Whitacre, 2018).

Traditionally, mainstream government and state corporations had not yet embraced remote working and emphasis were on physical appearance in offices for work. With the declaration of the Covid 19 as a pandemic by the World Health Organization (Cucinotta and Vanelli, 2020), organizations had to devise ways support the new arrangement with no time to prepare their

ICT infrastructure, put in place necessary security mechanisms and develop appropriate policies to guide accessibility of resources from remote locations. The expectation of the remote worker was that they would continue to execute their duties and responsibilities as though they were physically present at their places of work.

The pandemic instigated a new work from home culture around the globe with far-reaching technological implications including a stepped-up demand for ICT security solutions, Desktop as a Service (DaaS), Cloud computing, Virtual Private Networks (VPN's), and virtual desktop infrastructure (Borkovich and Skovira, 2020). It has resulted in important relevance for cybersecurity as it has brought to the fore long-standing security issues, and unheeded alerts that tend to define cybersecurity and at the same time creating a reliance on the Internet (Mohsin, 2020). (Mohsin, 2020) continues to argue that dependency on ICT technologies and the Internet creates vulnerabilities in cyberspace where malicious attempts proliferated to exploit this sudden, unplanned shift in organizations to operate online.

Public organizations are often blamed for cybersecurity breaches due to managements' reticence to recognize, plan and put in place adequate remote working measures, constantly analyze, scan, test, update, maintain ICT infrastructure and train employees to recognize and report pretexting overtures and cyberattacks, whether they are real or perceived (Borkovich and Skovira, 2020). Traditional cybersecurity strategies adopted are often vulnerable to inside threats due to the long-established practice that organizations and corporations have placed on perimeter security and thereby lacking the critical ability to detect and stop threats from within the network or system.

Cybersecurity provides protection from cyber threats for internet linked devices such as hardware, software and data where individuals and businesses employ cybersecurity measures to guard against illegal access to data and other electronic systems (Srinivas, Das and Kumar, 2019). A robust cyber security plan may offer excellent protection from hostile attacks aimed at accessing, altering, deleting, destroying, or extorting system and exfiltrating sensitive information of a company or user (Saleem, 2019). In combination with the rising numbers of users, devices, and applications in the contemporary business, many of which are sensitive or confidential, the significance of cyber security is still growing (Dearing, 2019). The increased number and complexity of cyber attackers and methods of assault exacerbate the issue.

Cybersecurity is a challenge for all businesses and organizations in a continuously changing threat environment. Traditional reactive approaches, in which resources were put toward protecting systems against the most severe known threats, while lesser-known threats were undefended, is no longer a sufficient tactic (Eastman, Versace, and Webber, 2015).

The changing and fluid nature of security threats is among the most challenging aspects for cyber security. New attack vectors are being created with the emergence of new technologies which are being utilized in new or different ways (MacIntyre, Engells, Scotch, Heslop, Gumel, Poste, Chen, Herche, Steinhöfel, Lim and Broom 2018). It may be difficult to keep up with the rapid changes and progress in attacks and to update procedures to defend against them (MacIntyre, 2018).

Remote work on the other hand is a flexible work arrangement that enables employees to work outside the office from a remote location (Felstead and Henseke, 2017). Secure remote work requires equipment management policies, network security and expectations for performance (Mandl and Biletta, 2018). Securing the remote work environment presents varied challenges from adversarial network attacks and insecure physical environments through to authentication and segmentation challenges, through to application layer security (Sharp, 2021). As such secure remote working with regard to cybersecurity refers to a situation where employees are able to execute their duties and responsibilities free from cyber threats or vulnerabilities as they establish connections from remote networks to ICT resources hosted on-premise or on the cloud.

Due to the coronavirus pandemic, remote work is becoming increasingly useful and vital for organizations. Its popularity grew when COVID-19 forced companies worldwide to send their workers to work virtually because of safety concerns (Caligiuri, De Cieri, Minbaeva, Verbeke and Zimmermann, 2020).

Statement of the Problem

Although there is substantial literature on the technological and cybersecurity threats and vulnerabilities, little research exists on how pandemics such as Covid-19 present opportunities for cybercriminals; with cybersecurity challenges estimated to cost USD 6 trillion a year worldwide by 2021, the number of the attacks has increased five-fold after Covid-19 pandemic (Williams et al., 2020).

In the haste establish the requisite ICT infrastructure to facilitate secure remote working as the pandemic raged on, cybersecurity was considered secondary to business continuity which was positioned at the forefront. Regrettably, cybercrime increased 600% since the commencement of COVID-19 (Lallie et al., 2021). Around 30% of businesses have observed an increase in cyber assault efforts since the pandemic began (Dwivedi et al., 2020). The increase in cyber-attacks was as a result of the sudden and abrupt shift of ICT resources to the cloud, use of online platforms and organizations embracing remote working where the commensurate cybersecurity measures are non-existent or inadequately implemented.

For financial regulatory state corporations in Kenya that adopted remote working where the conventional IT defense has been flipped on its head, the preparedness to protect remote workers from data and information security breaches, theft of credential data, ransomware, malware, phishing, and social engineering scams has been brought to question. Employees continue to access data, applications and management information systems from remote locations which has catapulted them to the front line of cybersecurity. Further, use of unsecured networks to access corporate systems, sharing of data and online collaborations has presented soft targets for cybercriminals to target and infiltrate with minimal visibility from the central ICT.

Research Objectives

The specific objectives included:

1. To investigate cybersecurity factors that influence secure remote working
2. To establish how cybersecurity preparedness, cybersecurity management procedures and cybersecurity threats affect remote working
3. To determine how cybersecurity models or frameworks influence remote working
4. To propose a model that demonstrates how different factors influence secure remote working
5. To validate the proposed model

Scope

This study was limited to the Financial Regulatory State Corporations in Kenya which include the Capital Markets Authority (CMA), Insurance Regulatory Authority (IRA) and the Retirements Benefits Authority (RBA) with the exception of Central Bank and SASSRA, within Nairobi. The sample population selected was limited to members of the ICT teams and selected users of management information systems enabled to work remotely for the respective organizations.

Significance of the Study

The researcher anticipated that management of the financial regulatory state corporations in Kenya and other stakeholders in cybersecurity management in Kenya will benefit from the resourcefulness of this study. The study is expected to generate interest among ICT stakeholders in both public and private organizations about the emergent cybersecurity issues, with a view to reworking current and existing strategies, frameworks and policies for securing their information assets and the remote worker during the Covid-19 pandemic and beyond.

This could be through development of new frameworks, policies or ICT governance models that propagate the confidentiality, integrity and availability of information resources in a more secure fashion with the remote worker at the center. Ultimately, the study intended to contribute to global knowledge on the impact of cybersecurity with the sudden adoption of remote working in Kenya.

Assumptions and Limitations of the Study

In conducting this study, the researcher made the assumptions that respondents will provide relevant and reliable responses, that the respondents had adopted the remote working concept in some form, and that there was a correlation between the remote workforce and increased cybersecurity challenges in the financial regulatory state corporations in Kenya.

CHAPTER TWO

2. 0 LITERATURE REVIEW

This chapter examined the empirical literature, which consisted summaries of similar studies performed across in Kenya and beyond. The literature comprised of a review and analysis of peer-reviewed journals, and academic publications acquired through online database sources and academic books.

COVID-19 pandemic and remote working

The COVID-19 pandemic brought about change at the workplace, and as a consequence increased teleworking, via faster digitalization and decentralisation of office operations. The worldwide reaction to the health crisis necessitated the development of alternative models of working, which in turn led to the need to offer new solutions to old concerns about remote working efficiency and cyber security. According to a Eurofound study, in the pre-pandemic era only 15% of EU workers had teleworking for at least once, whereas close to 40% had teleworking during the pandemic (Beno and Hvorecky, 2021; Mihailovic, Smolóvic, Radevic, Rašovic and Martinović, 2021). The number of teleworkers in the United States nearly doubled to 67% from mid-March to early April (Brenan, 2020).

In contrast, the rapid development of remote working raised questions about the preparedness of the technical ICT infrastructure, human skills and cybersecurity aspects of virtual workplaces. In addition to highlighting the fundamental issue of efficiency, the decentralisation of office operations, which occurred as the unavoidable result of teleworking, also emphasised the subject of its relationship to the cyber security of organizations. Studies revealed how the pandemic influenced the formation of the global remote work culture, given the worrying increase in security concerns (Mihailovic et al., 2021).

Employees that worked completely remotely may have had their connections isolated from the rest of the company's network increasing the lack of visibility by the central ICT and resulting in cybersecurity challenges where these connections were not adequately monitored. Hybrid employees (staff working on and off remotely) on the other hand, increased the attack vector every time they were physically present at the office and plugged their devices to the network, along with malware they may have unintentionally exposed themselves to (Tukur, Thakker and Awan, 2021). Cybercriminals may have obtained access to users, the network, and the company's data through compromised hosts (Tukur et al., 2021). Securing these access points, monitoring malicious activity, detecting, and preventing intruders, and recovering from the impact of attacks caused by cyber criminals is a daunting challenge for IT departments that complicates the hybrid work paradigm (Kimani, Oduol and Langat, 2019).

Cybersecurity threats and remote working

With between 50% and 90% of employees working remotely, companies were increasingly seeing remote work as the future mode of working (Bonacini, Gallo and Scicchitano, 2021). While remote work offers several advantages, the most significant challenge is cybersecurity. Businesses and organizations confront cybersecurity problems such as data protection, networking issues, and cloud computing risks (Bonacini et al., 2021). OpenVPN conducted research that revealed that 90% of IT experts believe that remote employees are not adequately secured (Balaji, 2019). Since each remote worker connects to a separate network that may be unsafe, employee security was a significant problem.

Working from home challenges included using public networks and personal devices, both of which have a plethora of security flaws. Another significant aspect at risk was organizational data where intentional or unintentional exposure may occur. Cybersecurity is a crucial issue for organizations, primarily since everything in today's corporations includes data. Without in-depth security, sensitive and private data is very vulnerable to abuse by unscrupulous people (Leuprecht, Skillicorn, and Tait, 2016). While system administrators, network engineers, and ethical developers deal with hardware and are thus familiar with security problems, while working from home, cybersecurity concerns were increasingly significant (Lin and Bergmann, 2016).

According to Georgiadou, Mouzakitis, and Askounis (2021), Tessian study showed that one-third of workers believed they can get away with riskier security practices while working remotely. Additionally, the study showed that almost 40% of respondents stated that their cybersecurity activity at home differs from their behaviour at work. Additionally, the majority of remote employees let family members to use business computers for personal use, and 82% of workers confess to password reuse. According to Bulpett (2020), nearly all IT executives (95%) see email as the main security issue to business data, yet employees usually rely significantly on email and messaging apps to communicate with colleagues and customers. While this behaviour is reasonable, it exposes companies to higher risks since the likelihood of clicking on an infected or socially engineered email rises in lockstep with the growth in email traffic. Additionally, when remote working, it may be difficult to authenticate the legitimacy of emails and their senders.

The findings demonstrate that cybersecurity threats have a direct impact on the ability of organizations to facilitate secure remote working. The coronavirus epidemic provided cybercriminals new attack vectors to target companies (Walters and Novak, 2021).

Cybersecurity Preparedness and Secure Remote Working

In many respects, the exceptional COVID-19 issue led to a big shift, where remote work became a trend to minimize viral expansion (Dwivedi, Hughes, Coombs, Constantiou, Duan, Edwards, Gupta, Lal, Misra, Prashant and Raman, 2020). Regardless of the size of the business, IT expenses were inevitable to sustain operations during the crisis (Dwivedi et al., 2020) whereas a result of regulatory and compliance requirements, the associated cybersecurity expenditure subsequently grew. Public organizations are often blamed for cybersecurity breaches due to managements' reticence to recognize, plan and put in place adequate remote working measures, constantly analyze, scan, test, update, maintain ICT infrastructure and train employees to recognize and report pretexting overtures and cyberattacks, whether they are real or perceived (Borkovich and Skovira, 2020). On the one side, the computer resources of companies are restricted to supporting remote work while workers often have not subscribed to sufficient firewall security and antivirus programs to operate remotely on their personal computers (Iakovakis, Xarhoulacos, Giovas, and Gritzalis, 2021).

Remote working significantly increased the likelihood of shadow IT usage, since the IT team can no longer adequately monitor devices and has no means of knowing what applications workers are using when away from the office or what activities they are engaged in, even if they believe they are installing something beneficial (Friess, 2016). Numerous tools became available on a freemium basis, which made them attractive to the uninformed. Bandos (2019) defined shadow IT as the usage of software or applications by workers that have not been authorized by the IT department. These kinds of applications or online tools may have vulnerabilities that hackers may exploit, putting the company at risk. Employees should be aware of how and where attacks may emanate from, as well as what activities may compromise their devices rendering them vulnerable to assault (Connolly and Wall, 2019).

Therefore, it is critical to train remote workers about cyber risks and how to avoid them, including how to recognize and react properly to social engineering and phishing efforts as an example, how to create secure passwords, how to physically safeguard their devices, and more

(Salahdine and Kaabouch, 2019). Research therefore revealed that preparedness of organizations to facilitate remote working and employee behavior had an influence on secure remote working. This research analyzed the direct connection between an organization's cybersecurity readiness and its workers' ability to work remotely in a secure fashion.

Cybersecurity Management Procedures and Secure Remote Working

The increased importance and relevance of ICT and the growth of the e-commerce industry have made cybersecurity a highly important policy issue worldwide (Kaur, Sharma and Singh, 2017). Ponsard, Grandclaudon and Dattons (2018) observed that cyber security tends to be ignored in favor of technical developments, while new risks to security are constantly exposed to cyber-attacks. Increased frequency and complexity of cyber security assaults throughout the sector have increased the cost of cyberattack mitigation and recovery (Watkins, 2013). Klaper and Hovy (2014) demonstrated that the effects of cyber security are especially crucial for governments. The new method of working increased the risk of cybersecurity attacks to employees working remotely to new vulnerabilities (Singer and Friedman, 2014). By expanding their digital footprints, businesses have the opportunity for sustainable innovation and performance but at the same time requiring enhanced measures to mitigate cybersecurity challenges (Golder and Macy, 2014).

Similar to compliance with HIPAA, PCI and IMO 2021, corporate cybersecurity policies should contain obligatory enforced standards (Webster, 2021). Retraining remote workers is key to enforcement since excellent practices are frequently forgotten after a short period of time. In addition to being aware of recommended practices, workers need periodic training to assist them detect spam and phishing assaults (Brotherston and Berlin, 2017). All devices utilized and linked should be equipped with antivirus, VPN, and anti-malware software, along with strong password requirement, according to (Ciesla 2020). A research of information technology security procedures, a case study of Kenyan small and medium businesses (SMEs) in the banking sector was conducted by Makumbi (2012). The study's goals were to determine how reliant Kenyan SMEs are on ICT, to determine the most common security threats among Kenyan SMEs, and to determine how Kenyan SMEs secure their computers, data, and networks from information security threats. The research found that the businesses examined were aware of the significance of information system security and had attempted to deploy security measures as a result of their dependence on IT systems.

Nyamongo (2012) investigated the security management of information systems at private chartered universities in Kenya. The research discovered that Kenyan institutions of higher learning were willing to embrace and enhance their information system security management by providing frequent security updates to management. Staff training in information security system management would enhance university's information security system management greatly. Malware, human error, computer theft, and system and software faults were identified as major risks confronting the information security system management. It was reasonable to infer that higher education institutions should reconsider their approaches to protecting their most valuable assets. As such, these institutions needed to develop an effective plan to enable them manage information security effectively. This research therefore will examine the direct connection between cybersecurity management procedures and secure remote working.

Theoretical Review of Literature

In context, information security and cyber security are critical because they concentrate on the level of protection that is optimal for an organization's information resources. According to a review of the literature, there are many theories on information security practises and cyber security, which include, Socio-technical System theory, Social Cognitive Theory, and Resource-Based View theory.

2.5.1 Socio-technical System theory

Emery and Trist (1960) developed the theory of socio-technical systems to characterise systems that include a complex interaction between people, machinery, and the environmental elements of a work system. Today, this relationship applies to most business systems. The theory of socioeconomic theory (STS) demonstrates how the social and technological elements of a working environment coincide and interact. The aim is to optimise both to ensure the smooth running of an organisation (Pasmore, Winby, Mohrman and Vanasse, 2019). STS theory highlights both the social and the technological elements of a company and considers both these characteristics to be interconnected (Sovacool and Hess, 2017).

Ideally, organizations aim to ensure collaborative optimisation is achieved. This implies that workplaces should be structured such that both people and technology complement each other, rather than just adopting current technologies. Socio-technical theory is based on the premise that understanding and improving the design and performance of any organisational system requires treating both 'social' and 'technical' elements as interconnected components of a complex system (Kapoor, Bigdeli, Dwivedi, Schroeder, Beltagui and Baines, 2021). Organizational transformation initiatives often fail because they are too focused on a single element of the system, most frequently technology, and fail to analyse and comprehend the system's intricate interdependencies (Baxter and Sommerville, 2011).

As technology advances daily, so does concern about the challenges associated with it (Westerman & Hunter, 2007). Information security, for example, requires management's attention. Within this perspective, information security risks are a component of sociotechnical systems that include human and technology elements. Therefore, when a security risk specifically targets a technological system, it has a cascading effect on the social and environmental systems. Thus, from an STS perspective, it was critical to assess and maintain compliance with social and organisational information security standards via the procedural design of safe STS. Specifically, ensuring that all components of STS (structure, people, and technology) are functioning optimally to protect critical information resources may result in increased security, efficiency, and performance. Technical, human, and organisational characteristics, as well as their interconnections, all contributed to the act of preserving and protecting information inside an organisation (Albrechtsen, 2007). As a result, this research considers security controls to be critical components of Socio-Technical Systems.

2.5.2 Social Cognitive Theory

Social Cognitive Theory (SCT) was deemed important to the research. Albert Bandura's Social Learning Theory (SLT) from the 1960s is now known as the Social Cognitive Theory (SCT) which asserts that there is a dynamic and reciprocal interplay between the person's surroundings, and his or her conduct, which is posited in the Social Context Theory (Bandura, and Walters, 1977). With its focus on social impact and social reinforcement, SCT is unique.

People's previous experiences are taken into consideration when determining whether they would behave in a certain way. All these factors affect whether a person will participate in a particular activity, as well as the reasons for engaging in that conduct (Azman, Samuel, and Osman, 2021). SCT describes human conduct as a trade and reciprocal interplay of personal variables, behaviour and the environment. The belief in one's own capacity to safeguard information and information systems against illegal disclosure, alteration, loss, destruction, and non-availability may be described as self-efficacy in information security (Rhee, Kim, and Ryu 2009). With regard to remote working, the employee’s self-efficacy is brough into question as factors surrounding their remote environment may determine how they will handle security of the information at their disposal.

2.5.3 Resource based view theory

Further, this study adopted the Resource Based View (Rumelt, 1984; Wernerfelt, 1984), which proposes that a firm's competitive advantage is based primarily on the application of a bundle of valuable tangible or intangible resources at the firm's disposal to portray the organization's agility characteristics. According to the resource-based perspective, businesses possess resources, a subset of which enables them to gain a competitive advantage and a subset of which results in better long-term performance (Lavie, 2006). Valuable and scarce resources may result in the development of a competitive advantage. This advantage may be maintained for extended periods of time to the degree that the company is able to safeguard against resource imitation, transfer, or replacement. By and large, empirical investigations based on the theory have significantly favoured the resource-based perspective (Datta, 2007).

In terms of information security, it is thought that organisations may maintain a competitive edge by making information resources confidential via measures that promote secrecy and security (Nelson & Romer, 1996). RBV indicates that a company's resources may comprise all assets, capabilities, organisational processes, firm characteristics, information, and knowledge that the firm controls and that allow the firm to devise and execute strategies that increase its efficiency and effectiveness (Barney, 1991). In this context, this research argued that information security is critical for safeguarding information resources (information systems) and using them strategically for competitive advantage.

Cybersecurity Models

CIS security controls

The CIS Critical Security Controls were developed by the Center for Internet Security as a prescriptive, prioritized collection of cybersecurity best practices and defensive measures that may aid in preventing widespread and severe attacks and ensuring compliance in a multi-framework age (Brotherston and Berlin, 2017). These actionable cyber defence best practices were developed by a group of IT professionals based on data collected from real attacks and their successful countermeasures (Skopik, Settanni and Fiedler, 2016).

The 20 CIS checks are divided into three categories: fundamental, foundational and organizational. Basic controls (Maennel, Mäses and Maennel) are often referred to as cyber hygiene controls. These controls concentrate on fundamental safety principles, including configuration management, vulnerability assessment and ongoing monitoring (Maennel et al., 2018). The second category, Foundational Controls, allows an organization to establish a foundation for a strong safety program. The latter category provides prescribes the relevance of people and processes (Thompson, 2017).

The CIS Measures are based on a consensus list of security controls that security professionals think and believe are the most effective defensive methods for preventing data breaches and minimising the risks of cyber assaults (Sadik, Ahmed, Sikos and Islam, 2020). The CIS measures also cover identifying indications of compromise and preventing further attacks in addition to stopping unwanted access (Sadik et al., 2020). The CIS controls identify defences for lowering the initial attack surface by hardening servers, detecting compromised computers, interrupting command-and-control or malicious software, and creating adaptive, continuous defences that are constantly enhanced (Wolff, 2016).

ISO 27001:2013

The worldwide standard for information security is ISO/IEC 27001:2013 (also known as ISO27001) lays the information security management system (ISMS) standard (Wanyonyi, 2020). The best practice approach of the ISMS standard enables organizations to manage information security by addressing people, processes and technology. The ISO 27001 Standard certification is recognized globally to show that your ISMS is consistent with best practice on information security (Calder, 2017). ISO 27001 is a framework that assists companies in establishing, implementing, operating, monitoring, reviewing, maintaining, and continuously improving an ISMS. It is part of the ISO 27000 family of information security standards (Haufe, Colomo-Palacios, Dzombeta, Brandis and Stantchev, 2016). An Information Security Management System (ISMS) is a method for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security based on a systematic business risk strategy (Haufe et al., 2016). It is an approach to information security that is taken by an organisation.

The ISO/IEC 27001:2013 standard defines the criteria for developing, implementing, maintaining, and continuously improving an information security management system inside an organisation. It also contains standards for assessing and treating information security threats that are specific to the organization's needs. The ISO/IEC 27001:2013 standards are general and designed to apply to all companies, regardless of form, size, or nature.

National Institute of Standards and Technology (NIST)

NIST's cybersecurity initiatives aim to promote the development and implementation of realistic, innovative security technologies and methods that will strengthen an organizations capacity to handle current and future computer and information security issues (Sittig et al., 2018). NIST provides cybersecurity standards, guidelines, best practices, and tools to suit the requirements of the United States' private sector, government agencies, and the general public. To enable organizations and businesses manage their cybersecurity risks, the Framework incorporates industry standards and best practices. It establishes a common vocabulary that enables employees at all levels of a company and across the supply chain to create a shared knowledge of their cybersecurity threats (Newhouse, Keith, Scribner and Witte, 2017). The

Framework not only assists companies in understanding their cybersecurity risks (threats, vulnerabilities, and consequences), but also in determining how to mitigate these risks via tailored solutions.

The above models and frameworks represent the cybersecurity best practices and how they influence organizations in facilitating secure remote working. Thus, in this research, these cybersecurity best practices and measures act as a controlling variable cybersecurity management procedures and secure remote working.

Summary of literature review

In the literature review researcher provided a summary of the cyber security challenges affecting organizations following the abrupt move towards remote work occasioned by the Covid 19 epidemic. While remote work as a concept provided some benefits to workers as demonstrated in the review of literature, the rapid and unexpected change to online work and remote access led to an increase in vulnerabilities and cyber security risks.

Literature revealed that human error was a major contributor to cyber risks in an organization. This was due to poor knowledge of existing and emergent cyber security risks, the abandonment of safety measures while working remotely and the vulnerability to social engineering assaults, which easily mislead the unsuspecting worker into paving the way for attacks. Further, use of personal devices increased the attack vectors since the required levels of security against current threats did not exist for the remote worker. Central ICT teams lost visibility for monitoring user behaviour and computer device security. Device management such as essential patches and upgrades and security settings became more complex due to the remote nature of devices. Since these devices were set for downloading central server security configurations, most devices operated unsecured.

Variable Definition and Hypothesis

Independent Variables

Cybersecurity Preparedness

This independent variable represented the cybersecurity state or posture of the financial regulators when they abruptly shifted their operations online to facilitate remote working. It highlights any measures that may or may not have been implemented at the time remote working was adopted causing an effect on the dependent variable – secure remote working.

Cybersecurity threats

This variable represented the risks and threats that negatively impacted the ability of the of the financial regulators in facilitating secure remote working.

Cybersecurity Management Procedures

This independent variable represented the activities, controls or defense measures that were necessary or required to facilitate secure remote working. It includes indicators such as cybersecurity policies that cover the remote worker, threat detection, protection and response measures, risk assessment and management procedures and device protection mechanisms.

Dependent Variable

Secure Remote Working

This variable represented the desired state for the financial state regulators in Kenya during Covid-19 and beyond when facilitating employees and other stakeholders to work from home. It includes indicators that define the required authentication and authorization, optimum levels of cybersecurity awareness, network, systems and application security controls, user activity and security event auditing to guarantee secure remote working.

Moderating Variable Implemented Cybersecurity Models

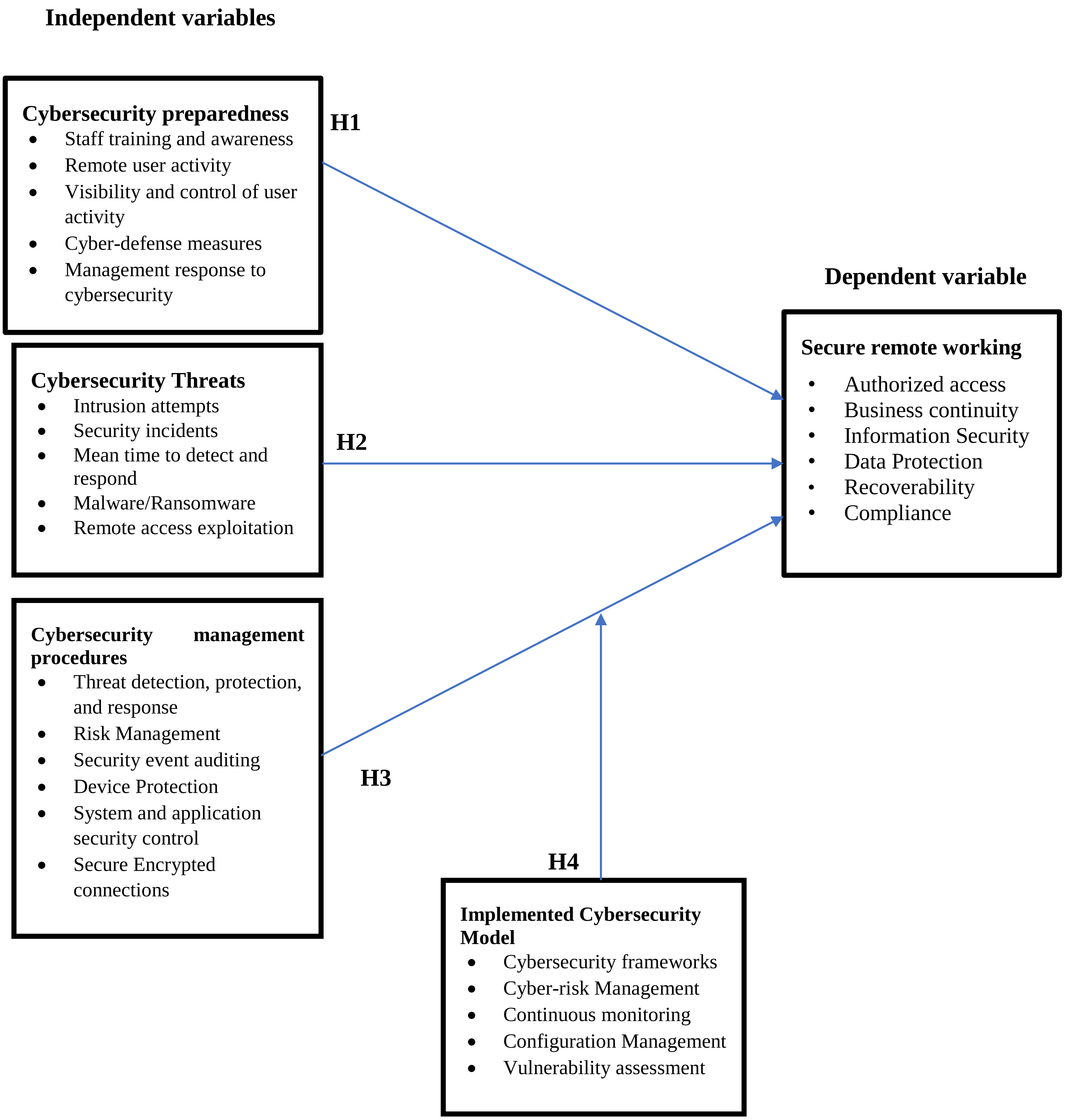
This variable moderated the influence of the independent variable (cybersecurity management procedures) on the dependent variable (secure remote working).

Conceptual framework

According to Imenda (2014), a conceptual framework is a set of interconnected constructs (theories) about the function or connection of a particular event. It establishes a basis for understanding the causation or correlation patterns of connections in events, ideas, observations, concepts, information, and interpretations, among others, by demonstrating the relationship between the independent and dependent variables.

The conceptual model for the research is shown in Figure 1 shows the dependent variable secure remote working is linked to the three independent variables. It demonstrates how cybersecurity preparedness, cybersecurity threats, and cybersecurity management procedures relate to influence a secure remote working environment. The moderating variable strengthened the association between independent (cybersecurity management procedures) and the dependent variable (secured remote working).

Figure 1: Conceptual Framework



Research Hypothesis

The thesis suggested the following general research hypothesis to describe the relationships illustrated in the conceptual model based on the theoretical and empirical literature review.

Hypothesis 1: Cybersecurity preparedness does not significantly influence secure remote working.

Hypothesis 2: Cybersecurity threats do not significantly influence or impact secure remote working**.**

Hypothesis 3: Cybersecurity management procedures do not significantly influence secure remote working.

Hypothesis 4: Implemented Cybersecurity Models do not significantly strengthen the effectiveness of cybersecurity management procedures for secure remote working.

Operationalization of the Conceptual Framework

Table 1 Operationalization of the Conceptual Framework

Variable Type	**Description**	**Indicators**	**Possible Measurement scale**	**Impact on the Dependent Variable**	**Literature Reviewed Papers**
Independent Variable Cybersecurity preparedness	This variable represents the cybersecurity state or posture of the financial regulators when they abruptly shifted their operations online to facilitate remote working. It highlights any measures that may or may not have been implemented at the time remote working was adopted causing effect on the dependent variable – secure remote working	• Staff training and awareness • Remote user activity • Visibility and control of user activity • Cyber-defense measures • Management response to cybersecurity	Ordinal Scale – 5 Five Point Likert scale Nominal Scale	Negatively impacts on the Dependent variable	(Antar, 2012). (Borkovich and Skovira, 2020) (Angafor, Yevseyeva, and He, 2020) (BaMaung et al., 2017) (Iakovakis, Xarhoulacos, Giovas, and Gritzalis, 2021)(Coventry and Branley, 2018) (Chapman 2020) (Serianu 2020) (BaMaung et al., 2017).
Independent Variable	This variable represents the activities, controls or defense measures that are necessary or required to facilitate secure remote working. It has a direct impact on the dependent	• Threat detection, protection, and response • Risk Management	Ordinal Scale – 5 Five Point Likert scale	Positively impacts on effective remote working	(Brotherston and Berlin, 2017).

Cybersecurity Management procedures	variable – secure remote working.	• Security event auditing • Device Protection • System and application security control • Secure Encrypted connections	Nominal Scale		Ciesla 2020
Independent Variable Cybersecurity threats	This variable represents the risks and threats that can exploit the cybersecurity preparedness of the financial regulators in facilitating secure remote working. It is a moderating variable between cybersecurity preparedness and secure remote working	• Intrusion attempts • Security incidents • Mean time to detect and respond • Malware/Ransomware • Remote access exploitation	Ordinal Scale – 5 Five Point Likert scale	Negatively impacts on the Dependent variable	(Kimani, Oduol, and Langat, 2019) (Eastman, Versace, and Webber, 2015). (Cybsafe, 2018) (Hatfield, 2019) (Sobers, 2017) (Dwivedi et al., 2020).
Moderating Variable Implemented Cybersecurity Models	This variable represents the cybersecurity best practices or industry standards based on the NIST framework, ISO/IEC 27001:2015 and CIS controls. It is a moderating variable where it positively influences both the cybersecurity management procedures and secure remote working.	• Cybersecurity frameworks • Cyber-risk Management • Continuous monitoring • Configuration Management • Vulnerability assessment	Ordinal Scale – 5 Five Point Likert scale	Positively impacts on the independent variable cybersecurity Management procedures	Radziwill and Benton (2017) Calder (2018) Thompson (2018)
Dependent Variable	This variable represents the desired state for the financial state regulators in Kenya during Covid-19 and beyond when facilitating employees and other stakeholders to work from home. It is the dependent variable that is affected or influenced by the manipulation of the independent variables.	• Authorized access • Business continuity • Information Security • Data Protection • Recoverability • Compliance			

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

A research study requires certain strategies, methods, and methodologies that vary according to the nature of the research issue and the researcher. The methodology that is chosen is influenced by the philosophical assumptions a researcher has about the actual world, knowledge, how information is acquired, and the techniques that will be utilized to collect, analyze, and interpret the data. This chapter describes the researcher's strategy and techniques for collecting, analyzing, and interpreting the data for the study.

Research Approach

The approaches to research are primarily classified as qualitative, quantitative, or combined. (Wanjohi, 2014) describes research methods as paradigms or frameworks that may be qualitative, quantitative, or a combination of the two, depending on the study design. The quantitative research approach is concerned with the researcher's need to quantify data using statistical or numerical methods and with building on existing theories through surveying or experimentation, whereas the qualitative research approach is concerned with an in-depth understanding of phenomena (Hkansson, 2013). Quantitative research approach was adopted. Quantitative research focuses on putting ideas and hypothesis to test, using statistical analyses and use of closed ended questionnaires.

Research design

Research design provides an appropriate framework or structure to guide the execution and analysis of data collected by the method of research (Sileyew, 2019). This is a type of inquiry in qualitative, quantitative, and mixed approaches that allow researchers to have a particular direction for research design processes (Ishtiaq, 2019). This study adopted the descriptive research design which is able to describe systematically and accurately the facts of a particular area of interest, describing what exists and what frequency with which something occurs. The study employed inferential statistics to explicitly show the associations or relationships between the independent, moderating, and dependent variables.

Sampling techniques and sample size

(Bhardwaj, 2019) describes sampling as a method used to choose a sample from a broad population to fulfill a certain research or study. In this study, a population refers to respondents with similar features, from whom the researcher selected subjects or samples. Representative samples were used to guarantee that the answers of one subgroup of the sampled population were not improperly exaggerated, disregarding the views of another fraction that may not be underrepresented but that balance is achieved.

The research focused on three financial regulatory state corporations in Kenya, with the exception of Central Bank of Kenya. The Capital Markets Authority (CMA), the Insurance Regulatory Authority (IRA) and the Retirement Benefits Authority (RBA). These three financial regulatory state corporations in Kenya constituted the analytical unit. The Observation Unit will consist of ICT teams, Market Conduct or Market Operations Directorates, and Finance team members or their equivalent personnel performing comparable responsibilities for each of these institutions.

The purpose of selecting the ICT, Market Conduct and Finance teams was to have the appropriate departments established by each regulatory agency. The ICT teams are solely responsible for the online use of infrastructures, business systems and applications and were considered to receive essential information about their readiness to operate online and are aware of the risks or vulnerabilities presented by the abrupt shift to remote work. Market conduct/operations and finance teams dealt with key infrastructures and systems such as information systems, ERP systems, market monitoring systems, among others, and thus their perspectives and experiences with cyber security issues during remote working are considered significant. The sample size was determined using the formula proposed by Yamane as shown below (Yamane, 1967):

$$n = \frac{N}{1+N(e)^2}$$

represent sample size, study population (100), and margin of error (5%) respectively. Where n, N, and e

The above equation was substituted to estimate the sample size (n) as illustrated below:

$$n = \frac{100}{1+100(0.05)^2}$$

$$n = \mathbf{80}$$

To achieve equitable distribution of the questionnaires, the staff complement within the ICT, Market Conduct and Finance departments was established at the respective State Corporations as below:

Table 2 Sample Population

Institution	Department Members	% of Population	Sample Size
CMA	ICT -	7.5%	6
	MARKET CONDUCT	22.5%	18
	FINANCE	8.75%	7
IRA	ICT	7.5%	6
	MARKET CONDUCT	17.5%	14
	FINANCE	7.5%	6
RBA	ICT	6.25%	5
	MARKET CONDUCT	15%	12
	FINANCE	7.5%	6
TOTAL		**100%**	**80**

Data collection

The data for this research was gathered via self-administered questionnaires, with close-ended questions being utilized. The questionnaire was split into parts to meet the research objectives of the study. The researcher sent out the questionnaires in google forms to respondents who had expressed willingness to participate. Only one submission per respondent was allowed. The respondents were assured of anonymity and confidentiality for the information they provided.

Data analysis

Descriptive statistics were used for the quantitative data to describe the sample data so as to portray the typical respondent and disclose the overall response pattern. It is a kind of data analysis that helps to explain, display, or summarize data points in a constructive manner so that patterns may develop that satisfy all of the data's conditions (Zeng, Arisona and Qu, 2013). Inferential statistics was employed to suggest explanations for a situation or phenomenon. It allowed the researcher to draw conclusions based on extrapolations, and make predictions based on data collected.

These statistics were produced using the Social Science Statistical Package (SPSS), which has a comprehensive data handling capability and numerous statistical analytical routines, capable of analyzing small to very large data statistics.

Validity and Reliability

Reliability of research instruments allows for consistent results. Supervision and monitoring of the data collection process was undertaken in order to ensure accuracy, completeness and consistency. Given that the key items captured by the questionnaire were on a Likert scale, the Cronbach’s alpha coefficient was used to test the instrument’s reliability. The acceptable reliability threshold was alpha coefficient equal to or greater than 0.7. The result of reliability statistics presented in table 3 below, the Cronbach alpha statistic was 0.757. Since the alpha coefficient was above the minimum acceptable threshold of 0.7, the questionnaire was considered a reliable research instrument that could be used to analyse the responses of the participants.

Table 3: Reliability Statistics

Cronbach's Alpha	**No of Items**
0.757	59

Ethical Consideration

Ethics apply to the established code of conduct and ensure that organizations involved in the investigation are not violated (Reed, Khoshnood, Blankenship and Fisher, 2014). This research was conducted for academic purposes, and this was made known to the respondents in the target population. The researcher received an introductory letter which clearly indicated the purpose of the research, and that the information was treated with utmost confidentiality. The researcher sought consent from respondents and advised them that their participation was voluntarily, their identity would remain anonymous, and privacy was safeguarded.

CHAPTER FOUR

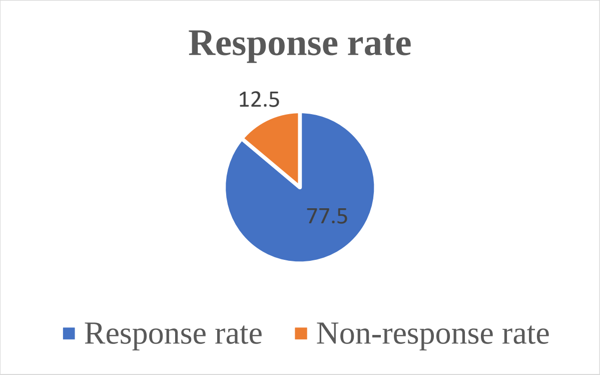
4.0 DATA ANALYSIS AND RESULTS

This chapter presents analysis of the collected data, interpretation and the presentation of the research findings so as to make meaningful deductions. Presentation of results was consistent with the objectives of the study and the conceptual framework. The analysis comprised of descriptive and inferential statistics. The findings were presented using tables, graphs and charts.

4.1.1 RESPONSE RATE

The questionnaires were administered online where only one submission was allowed per respondent. Out of the 80 online questionnaires distributed, 62 respondents were able to complete the survey, resulting to a 77.5 percent response rate. A sample response rate of 60% or more is considered satisfactory and can be utilized for analysis, according to Mugenda & Mugenda (2003). These finding is well illustrated in the Figure 4.2.1

Figure 2: Response rate



4.1.2 Demographic information

The research intended to elicit general information about the respondents in order to evaluate their fitness to participate in the study. The following subsections provide further information.

4.1.3 Cluster of organizations

The respondents were required to indicate the organization they worked for. The findings are represented in table 4.3.1 below.

Table 3 Cluster of organizations

Organization's name	**Frequency**	**Percentage**
Capital Markets Authority	24	38.7
Insurance Regulatory Authority	23	37.1
Retirements Benefits Authority	15	24.2
Total	**62**	**100.0**

Table 3 shows that 38.7% of respondents worked for the Capital Markets Authority, 37.1 percent worked for the Insurance Regulatory Authority, and 24.2 percent worked for the Retirement Benefits Authority. This result suggests the three financial regulatory institutions were involved, indicating that the data submitted was relevant and trustworthy for the research.

4.1.4 Department distribution

Respondents from the organizations were required to indicate the different departments they were stationed. The results are illustrated in table 4 below.

Table 4 Department distribution

Department	**Frequency**	**Percentage**
Market Operations/Conduct	34	54.8
ICT	16	25.8
Finance	12	19.4
Total	**62**	**100.0**

From table 4 above, it indicated that 54.8% of the respondents were stationed at the market operations/conduct department, while 25.8% were working at the ICT department and 19.4% of the respondents were working at the finance department. These departments represent the users in these state corporations that manage and maintain the enterprise systems in the case of the ICT department while Market Operations/Conduct and Finance departments heavily rely and use the enterprise systems to execute their mandates hence their perspective on cybersecurity and secure remote working was deemed paramount.

4.1.5 Level of education

The respondents were requested to state their highest educational level. Table 5 summarizes the results.

Table 5 Level of education

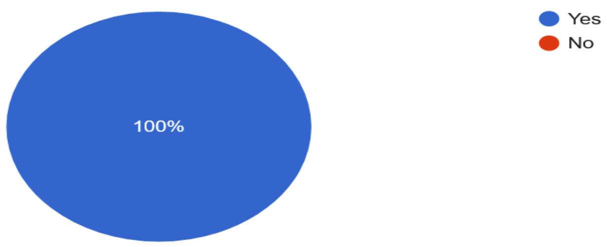
Highest level of education	Frequency	Percentage
Undergraduate	32	51.6
Post-Graduate	28	45.2
Diploma	2	3.2
Total	**62**	**100.0**

Table 5 showed that 3.2 percent of respondents had a diploma, 51.6 percent had an undergraduate degree, and 45.2 percent had a post-graduate degree. This meant that the majority of the respondents at Kenya's financial regulatory institutions had relevant basic understanding about cyber security, making it easier for them to answer the questions and offer accurate responses.

4.1.6 Remote Working Setup

At the onset of Covid-19, all the respondents of the three Regulatory Financial State Corporations indicated that the institutions had adopted remote working as depicted by Figure 3 below and therefore the data provided was relevant to the study.

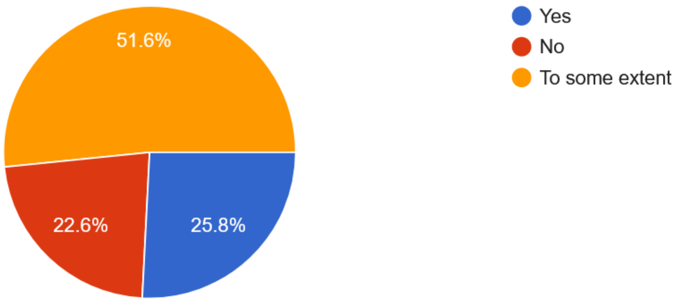
Figure 3 Remote working setup



4.1.7 Computing Device Assessment

With regards as to whether the institutions assessed the computing devices (whether provided by the organization or personally owned) to ensure secure remote working, results indicate that 25.8% claimed a thorough assessment was conducted, 51.6% of the respondents claimed that the assessment was conducted only to some extent, while 22.6% claimed no assessment was done. This meant that there was no standard methodology applied to determine the cyber-security state of the devices was employed to ensure secure remote working.

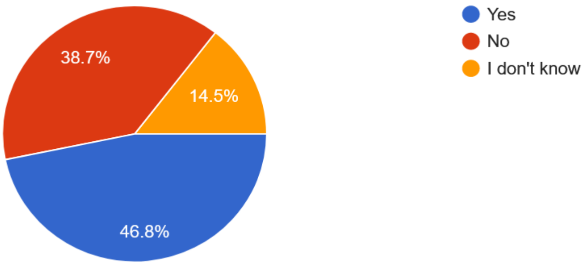
Figure 4 Computing Device Assessment



4.1.8 Administrative Privileges

On determining whether the respondents had administrative privileges on their devices, 46.8% claimed to have local administrative privileges on their devices, 38.7% did not have administrative privileges while 14.5% did not know whether they had the admin privileges or not. With a high number of users having local administrative privileges on their devices, in the event of a cyber-attack, then the possibility compromise and lateral movements was highly increased.

Figure 5 Administrative Privileges



4.0 Descriptive statistics

4.0.1 Cybersecurity preparedness in facilitating secure remote working during Covid-19 pandemic

In line with the first objective, the study sought to establish the effects of cybersecurity preparedness (security posture) in facilitating secure remote working during Covid-19 pandemic in Financial Regulatory State Corporations. The findings are presented in tables 4.4 and 4.5 below.

Table 6 Cybersecurity preparedness (security posture)

	Frequently	***Occasionally***	***I don't know***	***Rarely***	***Total***
How frequent does your organization update staff on cybersecurity threats and vulnerabilities during remote working?	*20(32.3%)*	*27(43.5%)*	*1(1.6%)*	*14(22.6%)*	*62(100%)*

	Very high	***High***	***Medium***	***Low***	***Total***
What is the level of cybersecurity awareness and sensitization in your organization?	*1(1.6%)*	*31(50(%)*	*26(41.9%)*	*4(6.5%)*	*62(100%)*

	Yes	***No***	***I don't know***	***Total***
Is there a standard docu mented process for on-boarding employees and providing access to ICT resources remotely?	*20(32.3%)*	*12(19.4%)*	*20(32.3%)*	*62(100%)*

	Strongly Disagree	***Disagree***	***Neither Agree nor Disagree***	***Agree***	***Strongly Agree***	***Total (%)***
The organization conducts a rigorous cyber security awareness and sensitization exercise during remote working	*0(0%)*	16(25.8%)	*22(35.5%)*	*24(38.7%)*	*0(0%)*	*Total 62(100%)*
Remote employees differ from office employees in their perceived levels of security, self-efficacy and compliance with relevant policies and practices.	2(3.25%)	*7(11.3%)*	*13(21%)*	*25(40.3%)*	*15(24.2%)*	*Total 62(100%)*
Your organization is finding it harder to administer cybersecurity measures during remote working	*2(3.25%)*	*9(14.55%)*	*26(41.9%)*	*20(32.3%)*	*5(8.1%)*	*Total 62(100%)*
Human error poses the greatest cybersecurity threat to the organization	*0(0%)*	*0(0%)*	*8(12.9%)*	*31(50%)*	*23(37.1%)*	*Total 62(100%)*
Our organization does not have adequate cyber-security framework, policy or procedures for remote workers	*1(1.6%)*	*15(24.2%)*	*23(37.1%)*	*19(30.6%)*	*4(6.5%)*	*Total 62(100%)*
Our organization has the capability to monitor remote user activity for cybersecurity threats	*3(4.8%)*	*20(32.3%)*	*19(30.6%)*	*19(30.6%)*	*1(1.6%)*	*Total 62(100%)*
Management has instituted measures to respond to cybersecurity threats during remote working	*0(0%)*	*8(12.9%)*	*29(46.8%)*	*24(38.7%)*	*1(1.6%)*	*Total 62(100%)*

Information on how prepared financial regulatory state corporations were in ensuring a secure remote working environment on the onset of Covid-19 was presented in Tables 6 above. Under it, upon engaging the respondents on how frequent their organization updated them on cybersecurity threats and vulnerabilities during remote working, 32.3% of the respondents stated that they frequently updated, 43.5% were occasionally updated, 1% had no idea and remaining 22.6% claimed that they were rarely updated.

On whether there was a standard documented process for on-boarding employees and providing access to ICT resources remotely, majority (32.3%) of the respondents stated that there was one, 19% declined and 32.2% of the remaining respondents had no idea of the existence of such a process. A majority 38.7% of the respondents agreed, 35.5% were indifferent while 25.8% disagreed with the fact that their organization conducted a rigorous cyber security awareness and sensitization exercise during remote working.

Nonetheless, 40.3% of the respondents agreed, 24.2% strongly agreed, 21% were indifferent, 11.3% disagreed and remaining 3.2% strongly disagreed with the fact that remote employees indeed differed from office employees in their perceived levels of security, self-efficacy and compliance with relevant policies and practices. On whether their organization found it harder to administer cybersecurity measures during remote working, a significant number 32.3% of the respondents agreed, 8.1% strongly agreed. 41.9% were indifferent, 14.6% disagreed and the remaining 3.2% strongly disagreed with the claim.

A majority (50%) of the respondents agreed, 37.1% strongly agreed while 12.9% were indifferent with the fact that human error posed the greatest cybersecurity threat to the organizations. With regard to the fact that, their organization didn’t have adequate cyber-security framework, policy or procedures for remote workers, 37.1% of the respondents were indifferent, 30.6% agreed, 6.5% strongly agreed, 24.2% disagreed and the remaining 1.6 % of the respondents Strongly disagreed with the claim.

Furthermore, 1.6% of the respondents strongly agreed, 30.6% agreed, 30.6% were indifferent,32.3% disagreed while 4.8% strongly disagreed with the fact their organization had the capability to monitor remote user activity for cybersecurity threats. Finally, a significant number (38.7%) of the respondents agreed, 1.6% strongly agreed, 46.8% were indifferent while the remaining 12.9% disagreed with fact that the management had instituted measures to respond to cybersecurity threats during remote working.

4.0.2 Cybersecurity management procedures in facilitating secure remote working during covid-19 pandemic

In line with the fourth specific objective, the study sought to establish the effects of cybersecurity management procedures in facilitating secure remote working during Covid-19 pandemic in Financial Regulatory State Corporations. The findings were according to table 7 below.

Table 7 Cybersecurity management procedures

	To a large extent	***Significantly***	***Insignificantly***	***Not at all***	***Don't know***	***Total***	
Is your organization able to monitor and control user/staff activity when they are working remotely?	*3(4.8%)*	*27(43.5%)*	*21(33.9%)*	*4(6.5%)*	*7(11.3%)*	*62(100%)*	
	Yes	***No***	***Only t some extent***	***Total***			
Is your organization able to monitor and control remote access connections from employees working remotely?	*18(29%)*	*7(11.3%)*	*37(59.7%)*	*62(100%)*			
	Yes	***No***	***Not sure***	***Total***			
Has your organization implemented any measures to detect, prevent and respond to cybersecurity threats encountered by staff as they work from home?	*21(33.9%)*	*0*	*41(66.1%)*	*62(100%)*			
	Weekly basis	***Monthly***	***Quarterly***	***Yearly***	***Never***	***Total***	
How often are cybersecurity awareness and sensitization trainings conducted for employees and stakeholders?	*0(0%)*	*3(4.8%)*	*29(46.8%)*	*25(40.3%)*	*5(8.1%)*	*62(100%)*	
	Strongly disagree	***Disagree***	***Neutral***	***Agree***	***Strongly agree***	***Total***	
User computing devices are constantly updated with latest patches, anti-malware tools, and security configurations.?	*0(0%)*	*11(17.7%)*	*29(46.8%)*	*20(32.3%)*	*2(3.2%)*	*62(100%)*	
	Quarterly	***Bi-annually***	***Yearly***	***Never***	***When need arises***	***Strongly agree***	***Total***
User computing devices are constantly updated with latest patches, anti-malware	*8(12.9%)*	*2(3.2%)*	*14(22.6%)*	*3(4.8%)*	*28(45.2%)*	*2(3.2%)*	*62(100%)*

tools, and security configurations.?				
	Yes	*No*	*Don’t know*	*Total*
Has your organization implemented identity and access management system such as Multi-Factor authentication for secure remote access?	*33(53.2%)*	*12(19.4%)*	*17(27.4%)*	*62(100%)*

A majority (66.1%) were not aware that their organization had implemented any measures to detect, prevent and respond to cybersecurity threats encountered by staff as they worked from home. The remaining 33.9% concurred with the claim.

Regarding how often cybersecurity awareness and sensitization trainings were conducted for employees and stakeholders, 4.8% of the respondents stated that it was conducted monthly, 46.8% quarterly, 40.3% yearly and the remaining 8.1% stated that it was never conducted.

Consequently, 17.7% disagreed, 46.8% were indifferent,32.3% agreed and the remaining 3.2% of the respondents strongly agreed with the fact that user computing devices were constantly updated with latest patches, anti-malware tools, and security configurations**.** Clearly, as stated by most (45.2%) respondents, user computing devices were constantly updated with latest patches, anti-malware tools, and security configurations only when need arose.

Additionally, crucial observations were made with regard to cybersecurity management frameworks and procedures put in place in facilitating secure remote working. The pertinent observations are outlined in figure 6 below.

Figure 6 Cybersecurity Management Measures Implemented for Secure remote working

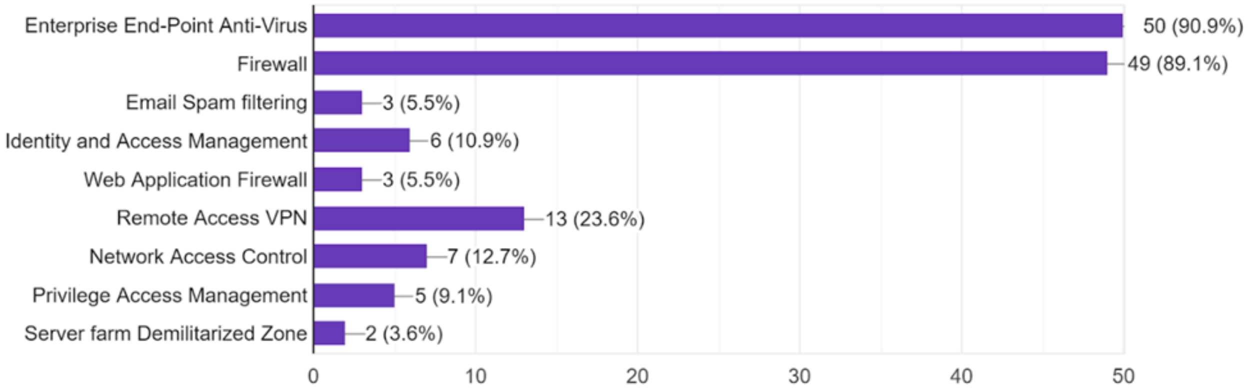
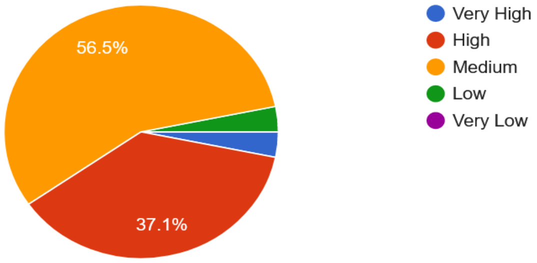


Figure 6 shows that 90.9% of the respondents claimed that enterprise End-point anti-virus was the most common measure put in place to protect their devices against cyber threats. 89.1% also agreed that their organizations had put in place a firewall to ensure a cyber-secure environment during remote working. Further, very few respondents claimed that their organizations had implemented the other cybersecurity measures such as email filtering, Identity and Access Management (IAM), a server farm demilitarized zone perhaps because they were unaware of such measures.

More insights were deduced on how effective implemented cybersecurity measure were. The results were according to figure 7 below:

Figure 7 Level of user device protection



From figure 7 above majority (56.5%) of the respondents claimed that the controls their institutions had implemented on their devices were at medium level while other respondents believed they were high (37.1%).

4.0.3 Cybersecurity threats experienced in facilitating secure remote working

In line with the second specific objective, the study sought to establish the effects of cybersecurity threats in facilitating secure remote working environment during Covid-19 pandemic. Data was analyzed and the findings presented.

Table 8 Cybersecurity effects on Secure remote working

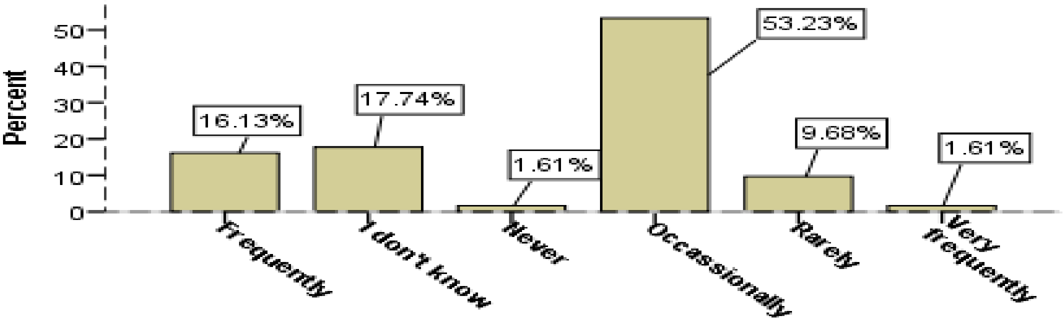
	Yes	***No***	***Not sure***	***Total***		
Have cybersecurity attacks been more frequent during remote working in the Covid-19 period?	*28(45.2%)*	*2(3.2%)*	*32(51.6%)*	*62(100%)*		
	Strongly disagree	***Disagree***	***Neutral***	***Agree***	***Strongly agree***	***Total***
Have cyber-attacks have become more sophisticated and dangerous in terms of negative consequences	*2(3.2%)*	*10(16.1%)*	*25(40.3%)*	*18(29.0%)*	*7(11.3%)*	*62(100%)*
	Strongly disagree	***Disagree***	***Neutral***	***Agree***	***Strongly agree***	***Total***
User computing devices are constantly updated with latest patches, anti-malware tools, and security configurations.?	*1(1.6%)*	*10(16.1%)*	*25(40.3%)*	*17(27.4%)*	*9(14.5%)*	*62(100%)*
	Strongly disagree	***Disagree***	***Neutral***	***Agree***	***Strongly agree***	***Total***
User computing devices are constantly updated with latest patches, anti-malware tools, and security configurations.?	*2(3.2%)*	*4(6.5%)*	*37(59.7%)*	*19(30.6%)*	*0(0%)*	*62(100%)*

Respondent's response on the cybersecurity threats experienced while facilitating secure remote working on the onset of Covid-19 was according to table 8 above. Under it, 45.2% of the respondents concurred, 3.2% objected while the remaining 51.6 % of the respondents were not sure whether cybersecurity attacks had been frequenting during remote working kin the Covid-19 period.

3.2% of the respondents strongly disagreed, 16.1% disagreed, 40.3% were indifferent, 29% agreed and 11.3% strongly disagreed with the fact that cyber-attacks had become more sophisticated and dangerous in terms of negative consequences. Furthermore, 1.6% of the respondents strongly disagreed, 16.1% disagreed, 40.3% were indifferent, 27.4% agreed while 14.5% strongly agreed with the fact that user computing devices were constantly updated with latest patches, anti-malware tools, and security configurations.

Additionally, information on the frequency in which attacks were experienced during the remotely working period was collected and presented on figure 8 below.

Fig 8 Frequency of attacks during the remotely working period



Insights from figure 8 above, depicted that majority of the respondents had experienced cybersecurity attacks occasionally.

Deductions were made regarding cybersecurity threats experienced in facilitating secure remote working together with what had accelerated them. The results were presented in table 9 below.

Table 9 Cybersecurity threats experienced

Threats	Frequency	Percentage
The threats your organization has encountered during the remote working period		
Phishing (email) campaigns and scams	50	80.6
Malware	37	59.7
Ransomware	36	58.1
Increased social engineering attacks	31	50
Remote access exploitation	5	8.1
I don't know	2	3.2
What has accelerated the cyber-attacks during remote working		
Sharing of computing devices (laptops) with other people while working from home	48	77.4
Use of unsecured network (WIFI/LAN) connections when working remotely	34	54.8
Relaxed or reduced levels of employee security and compliance when working remotely	28	45.2
Lack of critical and security updates and patches on computing devices when working remotely	28	45.2
Lack of employee cyber security awareness and sensitization	26	41.9

According to table 9, the organizations experienced several *cyber-threats* during the remote working period. 80.6 percent reported encountering some form of phishing campaigns and scams through email, while 59.7 percent reported encountering increased malware, and 58.1 percent reported encountering ransomware of some form. This does not imply that the threats were actualized but that they were encountered at some point.

The reasons provided that may have contributed to the increased cybersecurity issues included sharing of computing devices with other persons while working remotely with 77.4 percent stating as so, and 54.8 percent stated that using unsecured network (WIFI/LAN) connections while working remotely may have accelerated cyber-attacks in organizations. 41.9 percent indicated that a lack of cyber-security knowledge and sensitization among staff intensified cyber-attacks during the COVID-19 pandemic's remote working period.

Respondents were asked about their organizations' ability to administer cybersecurity measures and their views presented in figure 9 below.

Figure 9 Ability to administer cyber security measures

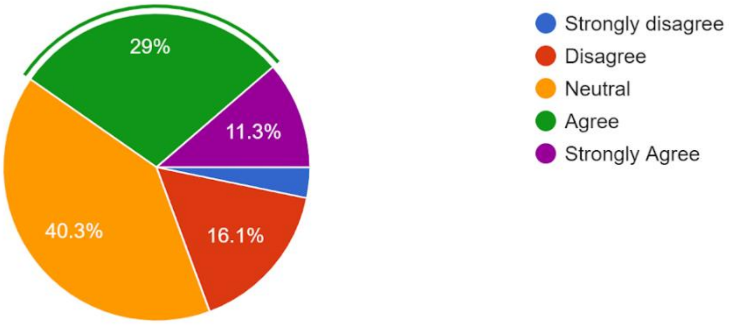
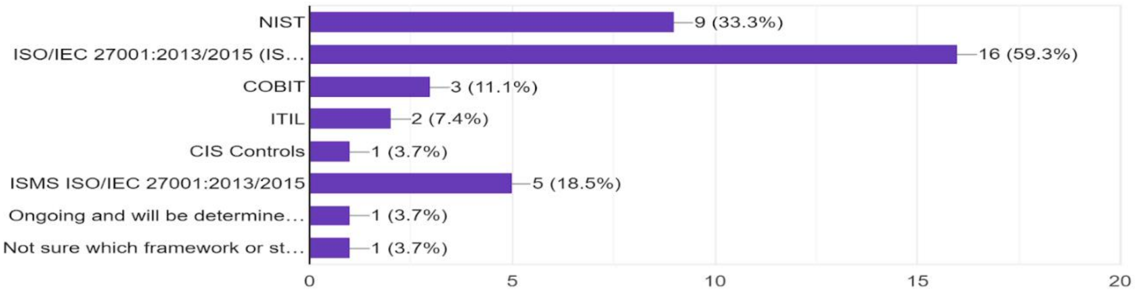


Figure 9 depicts the ability of the organizations to implement cyber-security measures during the remote working period. 11.3 percent and 29 percent of the respondents strongly agreed and agreed respectively that it was difficult for their organizations to implement cyber-security measures, while 40.3 percent of respondents said they were unsure how their organization were implementing cybersecurity measures. Perhaps this indicates that they did not have the requisite tools to do so. 16.1 and 3.2 percent disagreed and strongly disagreed that it was not difficult for organizations to implement the cybersecurity measures. This means that the three institutions had varied experiences in the implementing cyber-security measures during the remote working period indicating some had the mechanisms to institute measures while others did not have.

4.0.4 Implemented cybersecurity models

In line with the third specific objective, the study sought to investigate the characteristics of a cybersecure environment in facilitating secure remote working environment during Covid-19 pandemic in Financial Regulatory State Corporations. Data was analyzed and the findings presented as below.

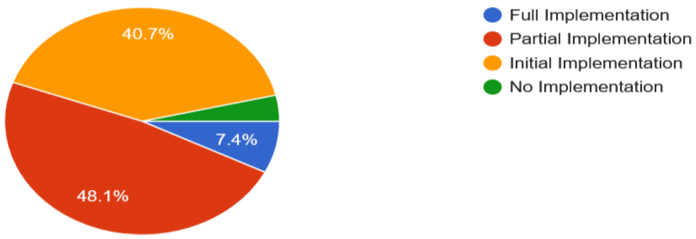
Figure 10 Cybersecurity management frameworks



From figure 10 above 33.3% of the respondents confirmed that their organization utilized the NIST framework as a cybersecurity management procedure in facilitating remote working. 59.3% indicated that their organizations used ISO 27001:2013, 11.1% indicated COBIT while 7.4% indicated ITIL and 3.7% indicated CIS control were used to facilitate remote working.

Additionally, insights made on cybersecurity management frameworks implementation were presented on figure 11 below.

Figure 11 Implementation of Cybersecurity Frameworks



However, with regard to the implementation of the above frameworks, 48.1% of the respondents indicated that only partial implementation had been achieved while 40.7% claimed that they were at the initial implementation of the adopted frameworks.

Finally, crucial observations were made with regard to implemented cybersecurity models. The pertinent observations are outlined in table 10 below.

Table 10 Implemented Cybersecurity models

	Yes	*No*	*Don't know*	*Total*
Has your organization adopted any framework, model or other methodology to enhance its cybersecurity posture?	*23(37.1%)*	*9(14.5%)*	*30(48.4%)*	*62(100%)*

	Yes	*No*	*I think so*	*To some extent*	*Total*
Does your organization have a comprehensive cybersecurity risk management framework	*16(25.8%)*	*7(11.3(%)*	*1(1.6%)*	*38(61.3%)*	*62(100%)*

	Yes	*No*	*Total*
The adoption of the framework or standard has improved the cybersecurity posture of the organization with regard to remote working.	*42(67.7%)*	*20(32.3%)*	*62(100%)*

	Yes	*No*	*Don't know*	*Total*
Has your organization adopted any framework, model or other methodology to enhance its cybersecurity posture?	*36(58.1%)*	*6(9.7%)*	*20(32.3%)*	*62(100%)*

Crucial additional information on cybersecurity implemented models was presented in table qo above. 37.1% of the respondents concurred, 14.5% objected while 48.4% confirmed to have no idea about their organization adopting any framework, model or other methodology to enhance its cybersecurity posture. Consequently, majority (61.3%) of the respondents confirmed their organization had to some extent employed some comprehensive cybersecurity risk management framework. 25.8% confirmed that the security measure had been implemented.

Majority (67.7%) of the respondents concurred with the fact that the adoption of the framework or standards had improved the cybersecurity posture of the organization with regard to remote working. 32.3% of them objected the claim. Finally, a significant number (58.1%) of the respondents confirmed that their organization had adopted at least one framework, model or other methodology to enhance its cybersecurity posture. 9.7% objected while 32.3% had no idea about the assertations.

4.0.5 Remote Working

The remote working environment adopted by the selected financial regulatory State Corporations was critically explored and the results presented in table 4.10 below.

Table 11 Remote working experience

	Yes	*No*	*Don't know*	*To some extent*	*Only some resources*	*Total (%)*
At the onset of Covid-19, did your organization adopt remote working or working from home?	*62100%)*	*0(0%)*	*0(0%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*

Were you facilitated with the requisite computing tools e.g. laptop, to enable you to work remotely?	56(90.3%)	*6(9.7%)*	*0(0%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*
Does your organization assess your computing device (personally owned or provided by your organization) to determine the security configurations and compliance level to security policies in place for remote working?	*16(25.8%)*	*14(22.6%)*	*0(0%)*	*32(51.6%)*	*0(0%)*	*Total* *62(100%)*
When working from home, are you able to access all ICT resources required to do your work as though you were physically present at the office	*46(74.2%)*	*2(3.2%)*	*0(0%)*	*0(0%)*	*14(22.6%)*	*Total* *62(100%)*
Do you have administrative privileges on your machines?	*29(46.8%)*	*24(38.7%)*	*9(14.5%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*
Are you able to alter or disable security systems installed on your provided computing tool when working remotely?	*26(41.9%)*	*23(37.1%)*	*0(0%)*	*13(21%%)*	*0(0%)*	*Total* *62(100%)*
Are you able to download and install software or alter the system configurations on your computing device when working remotely?	*34(54.8%)*	*28(45.2%)*	*0(0%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*
Do you use your computing device for personal use while working remotely?	*57(91.9%)*	*5(8.1%)*	*0(0%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*
Do you allow your family members to use your computing device when working remotely/working from home?	*27(43.5%)*	*35(56.5%)*	*0(0%)*	*0(0%)*	*0(0%)*	*Total* *62(100%)*

According to observations made as shown in table 11, it was confirmed by all respondents that at the onset of Covid-19, their organizations adopted remote working or working from home. A majority (90.3%) of the respondents confirmed that their organizations indeed provided them with the requisite computing tools to enable them work remotely on the onset of Covid-19. On whether their organizations did an assessment on their computing devices (personally owned or provided by their organizations) to determine the security configurations and compliance level to security policies in place for remote working, 25.8% of the respondents concurred with the claim, 22.6% objected while the remaining 51.6% confirmed that that it was to some extent done. Nevertheless, majority (74.2%) of the respondents concurred, 3.2% objected with the fact that they were able to access all ICT resources required to do their work remotely as though they were physically present at the office. 22.6% confirmed that they only able to access some resources and not all.

On whether they had administrative privileges on their machines, 46.8% confirmed that the indeed had, 38.7% objected while the remaining 14.5% didn't have an idea of whether the rights were extended to them or not. Consequently, 41.9% of the respondents confirmed that they were able to able to alter or disable security systems installed on their provided computing tools when working remotely. 37.1% objected the claim while 21% confirmed that they were to some extent able to alter the settings. Furthermore, 54.8% concurred that they were able to download and install software or alter the system configurations on their computing devices when working remotely. 45.2% objected the claim. Finally, majority (91.9%) of the respondents confirmed that they able to use their computing devices for personal use while working remotely.

4.1 Inferential Statistics

4.1.1 Correlation Analysis

A correlation test of association was run to determine the relationship existing between the study's independent variables (cybersecurity preparedness, cybersecurity management procedures, and cybersecurity threats) with the study's' dependent variable (secure remote working).

The correlation takes on values in the range of negative one (-1) to positive one (+1). The sign of the correlation coefficient indicates the direction of the relationship, while the magnitude of the correlation (how close it is to -1 or +1) indicates the strength of the relationship. The further the correlation is from either -1 or 1, or the closer it is to zero (0) the weaker the relationship and vice versa.

Table 12 Correlations Analysis

Variables		**Remote working**
Remote Working	Pearson C0rrelation Sig. (2-tailed) p-value N (Respondents)	1 62

Cybersecurity Preparedness	Pearson C0rrelation Sig. (2-tailed) N	-.210* .047 62
Cybersecurity management procedures	Pearson C0rrelation Sig. (2-tailed) N	.610 * .006 62
Cybersecurity threats	Pearson C0rrelation Sig. (2-tailed) N	. - .370* .035 62
Interaction	Pearson C0rrelation Sig. (2-tailed) N	.770* .001 62

**Interaction = Standardized (Zscore) cybersecurity management procedures multiplied by Standardized (Zscore) Implemented cybersecurity models

**. Correlation is significant at the 0.05 level (2-tailed)

Table 12 results revealed that, there existed a positive, perfect linear relationship (r = 1) between secure remote working and itself implying that a variable is perfectly correlated to itself.

The results also revealed a weak negative but significant linear relationship between cybersecurity preparedness and secure remote working **(r = - 0.21, p-value = 0.047),** leading to the rejection of hypothesis H1 and the conclusion that cybersecurity preparedness did indeed influence secure remote working.

Consequently, results revealed a moderate and negative but significant linear **association (r = -0.370, p-value = 0.035)** between cybersecurity threats and secure remote working, leading to the decision to reject hypothesis H2 and the conclusion that cybersecurity threats do indeed significantly influence secure remote working.

Similarly, results revealed a strong and significant positive linear association between cybersecurity management procedures and secure remote working **(r = 0.610, p-value = 0.006).** The findings led to the decision to reject hypothesis H3, resulting in the conclusion that cybersecurity management practices had a significant influence on secure remote working.

Finally, the findings revealed a strong positive significant linear relationship between the interaction (Interaction = Standardized (Zscore) cybersecurity management procedures multiplied by Standardized (Zscore) Implemented cybersecurity models) and secure remote working **(r = 0.770, p-value = 0.001).** As a result, hypothesis H4 was rejected, and the conclusion arrived that, indeed, implemented cybersecurity models significantly strengthened the effectiveness of cybersecurity management procedures to achieve secure remote working.

4.1.2 Regression Analysis

To determine the effects of the independent variables (Cybersecurity preparedness, cybersecurity management procedures, cybersecurity threats) and the moderating variable (Implemented Cybersecurity models) on the dependent variable (secure remote working), a multiple linear regression was run, and the results were presented as below.

Table 13 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	0.707[a]	.501	.164	0.63443

Table 13 revealed that; **R = 0.707**, it is the correlation coefficient between study’s independent variables, moderating variable, and the dependent variable. The results implied that there existed a strong, positive linear association between independent variables, moderating variable, and the dependent variable.

R-square = 0.501 is the coefficient of determination (effect size). The results imply that 50.1% of the variation on the dependent variable is explained by the independent variables while 49.9% is explained by variables outside the model.

Table 15 Regression Model

Model	Unstandardized Coefficients		Standardized Coefficients	Sig(p-value)	Collinearity Statistics	
	B	Std. Error	Beta		Tolerance	VIF
Constant	-1.080	.982		.105		
Cybersecurity Preparedness	- .630	**.287**	.261	.047	.545	1.836
Cybersecurity Threats	-2.142	.149	.104	.005	.564	1.774

Cybersecurity management procedures (Zscore)	2.709	.162	.225	.012	.951	1.052
Implemented Cybersecurity Models (Zscore)	1.013	0.141	.162	.041	.422	2.371
Interaction	.992	.163	.290	.011	.734	1.362

****Interaction = Standardized (Zscore) cybersecurity management procedures multiplied by Standardized (Zscore) Implemented cybersecurity models**

The Model was graphically visualized as below.

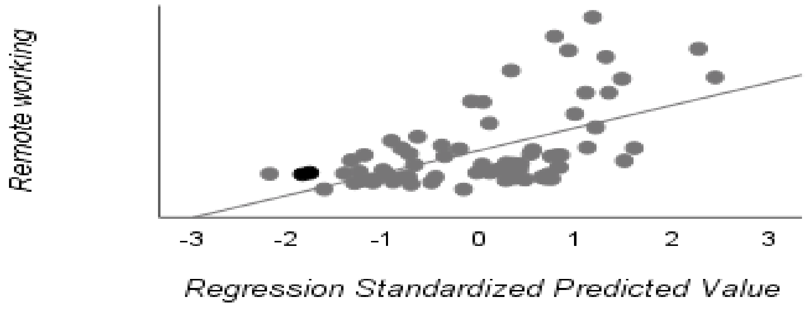


Figure 12: Regression model

Table 15 above represents the regression model which can be expressed as:

$$Y = \beta_0 - \beta_1 X_1 - \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + X_3 X_4 + \sum_x ,$$

$$Y = -1.080 - .261X_1 - .104X_2 + .225X_3 + .162X_4 + .290 + \sum_x$$ **Where:**

Y = Dependent variable (Secure Remote Working)

β_0 = - 1.080 (intercept)

X_1 = Cybersecurity preparedness

X_2 = Cybersecurity threats

X_3 = Cybersecurity management procedures

X_4 = Implemented Cybersecurity Models

X_3X_4 = Interaction

$\sum_x$ = Error term (disturbance term - Caters for missing data)

The results of the regression analysis model were presented in table 15 above. The findings revealed no severe multicollinearity between the study's independent variables and the moderator variable **[Variance Inflation Factor (VIF) < 4**].

To explain the effects of each independent variable on the dependent variable, the report was based on standardized beta coefficients. The standardized beta coefficient compares the strength and effect of each individual independent variable to the dependent variable.

From the regression analysis results in table 15 above, the independent variables [cybersecurity preparedness (p-value = 0.047), cybersecurity management procedures (p value = 0.012), cybersecurity threats (p value – 0.005) and the moderator variable (p value = 0.0.41)] we are all determined to be statistically effective in influencing the remote working environment.

The results further revealed that when cybersecurity preparedness measures had not been put in place or ignored by the financial regulatory state institutions under investigation, this had a negative significant (β_1= -0.261, p-value = 0.047) impact on the organizations ability to guarantee a secure remote working environment hence making its remote workers vulnerable. This was based on the assumption that cybersecurity threats, cybersecurity management procedures and the moderator variable (implemented cybersecurity models) were all held constant.

Similarly, any cybersecurity threats encountered by remote workers from any of the three institutions investigated there was a negative significant influence on the organization's ability to provide a secure remote working environment to its remote employees (β2 = - 0.104, p-value = 0.005). This was also based on the assumption that cybersecurity preparedness, cybersecurity management practices, and the moderator variable (implemented cybersecurity models) would all remain constant.

Further, assuming that cybersecurity preparedness and cybersecurity threats were held constant, results revealed that any additional cybersecurity management procedure employed by any of the three organizations under consideration had a positive significant effect on the organization's ability to guarantee a secure remote working environment to its remote workers (β3 = 0.225, p-value = 0.012).

Finally, the findings revealed a significant interaction (p-value = 0.011**)** between the moderator variable (Implemented cybersecurity models) and cybersecurity management procedures. The implication was that any cybersecurity model implemented significantly enhanced the cybersecurity management procedures, thereby enhancing an organization's ability to guarantee a secure remote working environment.

5.0 SUMMARY, DISCUSSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the key findings as per the set objectives. It includes the discussion of the results and presents conclusions drawn and the recommendations for the study. It also highlights the key areas for further research.

5.2 Summary of the findings

The response rate was the very first step in the data analysis. A response rate of over 77% was achieved and hence the questionnaires were considered satisfactory for analysis. Regarding cluster distribution, majority (38.7%) of the respondents were drawn from the Capital Markets Authority, followed by Insurance Regulatory Authority (37.1%) and the least (24.2%) drawn from the Retirement Benefits Authority. In terms of remote working adoption, all organizations reported doing so, with the market conduct department accounting for the majority (54.8 %) of employees. Similarly, some staff were provided with computing devices, while others were permitted to use their own. 51.6% of employees said the organization examined the devices to some extent to mitigate cybersecurity hazards. Finally, 46.8% of employees, the majority (51.6%) of whom were undergraduates, said they had been extended administrative privileges to their computing devices.

Factors that Influence secure remote working

In the cybersecurity assessment and from the literature review in this study, preparedness of organizations to facilitate secure remote working, cybersecurity management procedures or processes put in place or missing, cybersecurity threats that proliferated during the COVID-19 period that occasioned abrupt remote working and implemented cybersecurity frameworks or models were determined to be some of the significant factors that would influence or have a negative or positive correlation to secure remote working.

Cybersecurity preparedness and secure remote working

The study's **second objective** was to establish the institutions' level of preparedness at the time they adopted remote working, and several aspects were assessed. Staff training and awareness, remote user activity, cybersecurity defence measures in place, and management response to cybersecurity were among the themes explored. Based on the results, there was a relatively high level of cybersecurity awareness with 50% of the respondents claiming so and this was augmented by the fact that the institutions updated staff on cybersecurity threats and vulnerabilities during remote working.

However, there was no standard on-boarding process for enabling staff to work remotely where mixed results were observed with 32.3% claiming they guided on how to access resources securely while 32.3% were not and 19.4% were not aware of such a program. Over 50% and 37.1% of the respondents agreed and strongly that human error posed as the greatest cyber threat to the organizations respectively.

Literature review revealed that employees believe that they can get away with riskier security practices while working remotely according to Georgiadou, Mouzakitis, and Askounis (2021). These employees took up poor cybersecurity habits as they believed their ICT departments were not monitoring them. A considerable number of respondents (32.3 %) disagreed that their organization had the capability to monitor remote user activities for cybersecurity threats.

Cybersecurity management procedures and Secure remote working

With regard to the effects of cybersecurity management procedures in facilitating secure remote working, the results reveled that organizations had not implemented any measures to detect, prevent or respond to cybersecurity threats encountered by staff as they worked remotely with 66.1% claiming so. This was substantiated by the fact that the organizations were only able to monitor and control remote access connections of the employees to some extent with 59.7% affirming this.

Implemented cybersecurity measures not highly effective with 75.8% responding to confirm this as this organizations had majored only on relying on a Firewall and an enterprise anti-virus for the cybersecurity measures. Further, respondents (56.5%) claimed that the controls implemented at their devices resulted in medium levels of protection from cyber threats. It is only one institution that had put in place multi-factor authentication to secure remote access connections.

Cybersecurity threats and Secure remote working

Intrusion attempts, mean time to identify and respond to emergencies, and remote access exploitation were all examined to uncover cybersecurity threats encountered by remote working employees. These were analyzed based on the **second objective** of establishing the effects of cybersecurity threats experienced in facilitating remote working. The results indicated that a 51.6% of respondents agreed that cybersecurity breaches had gotten more sophisticated and dangerous. Similarly, phishing campaigns and scams via email, and an increase in malware proliferation were the dominant threats encountered with 80.6% and 59.7% respectively. However, the results further revealed that cyber threats were not as frequent and were only experienced occasionally with 53.23% affirming this.

Use of unsecured network (WIFI/LAN) connections and a lack of cybersecurity knowledge or awareness or sensitization while working remotely was cited by 54.8 % and 41.9% respectively as a factor in exacerbating cyber-threats in organizations. Further, lack of requisite security updates and required security policies exposed these devices to threats and vulnerabilities. As a result, organizations that were unable to monitor and control the security aspects of their devices found it more difficult to safeguard them. According to literature, without in-depth cybersecurity measures, sensitive infrastructure and data is very vulnerable to abuse (Leuprecht, Skillicorn, and Tait, 2016). According to Bulpett (2020), nearly all IT executives (95%) see email as the main security issue to business data, and this is confirmed by the results above where phishing attacks were reported as the main attack vector through email.

Cybersecurity Models and Secure Remote Working

Based on the regression model, cybersecurity frameworks greatly enhanced the cybersecurity posture of the financial regulatory institutions to achieve secure remote working. This is because where an organization had implemented a cybersecurity model or framework such as such as the National Institute of Standards and Technology (NIST), ISO 27001-2015, CIS Controls, COBIT etc., they had a significant positive effect on the implement cybersecurity management procedures or processes that resulted in an enhanced secure remote working environment. Though majority (67.7%) of the respondents concurred with the fact that the adoption of the framework or standards had improved the cybersecurity posture of the organization with regard to remote working none of the assessed organizations had fully implemented all the requirements of a framework. This meant that where a full implementation was achieved, then the resultant would be a significant enhancement of the remote working environment.

Proposed Model that demonstrates how different factor influence secure remote working

For the financial regulatory institutions and organizations at large to achieve a secure remote working environment, a host of measures need to be put in place. The fourth objective of this research study was to propose a model that demonstrates how different factors can achieve or results in a secure remote working environment. This proposed model was derived from the regression analysis model which revealed that the identified factors were significantly effective in enhancing and achieving a secure remote working environment.

This study conducted a cybersecurity assessment of the remote working environment where salient factors were established that influence the security of data, systems and applications as employees abruptly adopted working from home. These were cybersecurity preparedness, cybersecurity management procedures and cybersecurity models. The processes and activities that enhance an organization’s ability to bolster its preparedness to facilitate secure remote working included comprehensive training and awareness of staff and stakeholders on current and emergent cybersecurity threats, thorough computing and mobile device assessments before authentication and authorization to access resources remotely and enhancement device protection and establishment of a structured on-boarding program that takes staff and stakeholders through the processes of accessing resources remotely.

Further, organizations need to put in place cyber security management processes and activities to achieve a secure remote working environment. As was demonstrated by the regression model, where cyber security management procedures were implemented, this had a significant positive effect on the remote working environment. As such threat detection, response and protection, data and communication encryption, comprehensive security events auditing, and multi-factor authentication were some of the procedures that an organization needs to adopt.

To augment the above factors, the financial regulatory institutions and organizations need to adopt and fully implement a standard cybersecurity framework or model such as the National Institute of Standards and Technology (NIST), ISO 27001-2015, CIS Controls, COBIT among others. These frameworks should be specific to cybersecurity. Based on the regression model, cybersecurity frameworks greatly enhanced the cybersecurity posture of the financial regulatory institutions to achieve secure remote working.

This study proposes a model that demonstrates how these three factors need to be implemented in tandem to ensure a secure remote working environment. Where one aspect is not present, this will compromise the ability of organizations to achieve an optimum level of secure remote working. For an organization to achieve secure remote working, it needs to institute measures that enhance its preparedness. At the same time, management measures that address cybersecurity risks need to be adopted to increase the ability of an organization to guarantee a secure remote working environment. Finally, a standard framework or model to augment the cybersecurity practices of the preceding two factors is required so that an organization can be achieve secure remote working.

5.3 Discussion of Findings

From the analysis of the findings, the results indicated that the cybersecurity preparedness, cybersecurity management procedures, cybersecurity threats and adoption of cybersecurity framework or model by the financial regulatory state corporations were significant in achieving a secure remote working environment. The study demonstrated significant correlations among the independent variables to the dependent variable as well as the impact or effect of the moderating variable.

In line with the Socio-Technical Theory (STS) which opines that both the social and technological elements within an organization are interconnected, the results suggested that the abrupt shift to remote working occasioned by COVID-19 had a significant impact on the financial regulatory state corporations as employees and stakeholders demonstrated poor cybersecurity habits when working remotely.

Contrary to the hypothesized associations between the study’s independent and dependent variables, the results revealed significant influences on the organizations ability to facilitate secure remote working. The study analyzed the effects of the cybersecurity management process, and cybersecurity preparedness which all were determined to have a significant impact on the ability of organizations to achieve secure remote working. The observation was that where organizations did not have strong measures put in place, secure remote working was not possible, and the inverse was also true.

According to San Murugesan (2020), an organization's ability to effectively respond to a disruption is determined not only by how effective it was in the planning process, but also by how effective it was in its preparation, trials, and staff training, which is often overlooked. Furthermore, he asserts that infectious disease outbreaks and other forms of crisis, both anticipated and unexpected, are inevitable. Their impact, however, can be mitigated through better preparedness and more effective responses.

The study analyzed the effects of the cybersecurity threats on the state corporation’s ability to facilitate to secure remote working which was the third objective of this study. These all had a negative influence as more threats proliferated the remote environment became twice insecure. Interestingly, the research findings revealed that cyber threats were not as frequent and were only experienced occasionally. This contracted existing literature where Lallie et al., 2021 claimed that cybercrime had increased 600% since advent of COVID-19 and that 30% of business had observed an increase in cyber-attacks (Dwivedi et al., 2020). This could mean that the sampled organizations did not have the ability or requisite tools to monitor and detect cyber-attacks against them which made it difficult to defend against.

The existing cybersecurity framework or models are more focused on wholistic cybersecurity management measures and not specific to remote working. This study proposed a model that demonstrates how the identified factors interplay to influence and achieve a secure remote working environment. Whilst the study revealed a significant impact of frameworks and models to enhance the cybersecurity posture of the financial regulatory state corporations for secure remote working, the model proposed a three-pronged approach that encompasses the remote worker and their activities. This meant that the model is concerned with how prepared an organisation is to support the remote worker, what measures the organisation has put in place to protect the remote worker against cyber threats and adoption of model that augments these two aspects.

The results of this study do not challenge existing theories and build the on existing body of knowledge, therefore they should be considered where organizations have adopted remote working and intend to continue with this mode of work arrangement beyond COVID-19. However, the generalizability of the results may have been limited by the sample size though this was not determined to impact on their validity. The study also focused on three independent variables that impacted on secure remote working as the dependent variable and this may have limited the scope of the study as there may have been other factors that out of scope.

5.4 Conclusions

This research was concerned with undertaking a cybersecurity assessment of the remote working environment occasioned by the COVID-19 pandemic that resulted in the abrupt shift to working from home and online. After identifying and investigating the factors that significantly influence secure remote working, this study proposed a model that demonstrates how these factors interplay to positively influence the remote working environment for the financial regulatory institutions in Kenya during the Covid-19 period and beyond. Before the advent of the Covid-19 pandemic, government entities, organizations and businesses did not have a model, policy or framework in place that covered remote working. Instead, the cybersecurity designs were centralized and focused on the perimeter defenses.

The cybersecurity assessment affirmed that organizations needed to enhance their preparedness to facilitate a secure remote working environment, undertake cybersecurity management processes that increase their ability to identify and addresses current and emergent cybersecurity threats and support the adoption of an established framework that can improve the security of the remote working environment.

The proposed model demonstrated the different factors or aspects that are required for an organization to achieve secure remote working. This was based on the regression analysis that revealed how significant cybersecurity preparedness, cybersecurity management procedures and cybersecurity frameworks were statistically effective in positively influencing the remote working environment to prevent cyber threats. The measures that an organization should put in place to address its preparedness, cybersecurity management processes and adoption of a standard framework to augment these measures were highlighted as fundamental activities to achieve the desired state of cybersecurity for remote working.

State corporations in Kenya that have adopted the remote working culture either fully or partially can utilize these research findings to establish a common cybersecurity strategy to respond to cybersecurity risks that arise due to the remoteness of their employees and stakeholders. They can be used to enhance existing strategies already in place to improve the cybersecurity posture of organizations.

5.5 Recommendations

The following recommendations were made after the findings and statistical analysis of this study:

(i) Development of a model that can be used to mitigate cybersecurity threats occasioned by the new work from home arrangement as a result of the Covid-19 pandemic.

(ii) The ICT Authority charged with the responsibility of rationalizing and streamlining the management of all Government of Kenya ICT functions should consider developing policy guidelines that define how the remote worker can be secured for adoption by both public and private entities.

(iii) Further assessment of the variables outside of this study that may significantly influence the security of information and data during remote working.

REFERENCES

Antonucci, D., 2017. *The Cyber Risk Handbook: Creating And Measuring Effective Cybersecurity Capabilities*. John Wiley & Sons.

Abulibdeh, A., 2020. Can COVID-19 Mitigation Measures Promote Telework Practices?. *Journal Of Labor And Society*, *23*(4), Pp.551-576.

Ahmad, N., Amer, N.T., Qutaifan, F. And Alhilali, A., 2013. Technology Adoption Model And A Road Map To Successful Implementation Of ITIL. *Journal Of Enterprise Information Management*.

Akin, L. & Gözel, M. G. 2020. Understanding Dynamics Of Pandemics. *Turkish Journal Of Medical Sciences,* 50**,** 515-519.

Albrechtsen, E., 2007. A Qualitative Study Of Users' View On Information Security. *Computers & Security*, *26*(4), Pp.276-289.

Ali, M. & KauR, D. 2020. Byod Cyber Forensic Eco-System. *International Journal Of Advanced Research In Engineering And Technology (IJARET),* 11.

Al-Turjman, F. And Salama, R., 2021. Cyber Security In Mobile Social Networks. In *Security In Iot Social Networks* (Pp. 55-81). Academic Press.

Amoroso, E. 2006. *Cyber Security* Silicom Press.

Andrade, R. O., Ortiz-garcés, I. & Cazares, M. Cybersecurity Attacks On Smart Home During Covid-19 Pandemic. 2020 Fourth World Conference On Smart Trends In Systems, Security And Sustainability (Worlds4), 2020. IEEE, 398-404.

Angafor, G.N., Yevseyeva, I. And He, Y., 2020, November. Bridging The Cyber Security Skills Gap: Using Tabletop Exercises To Solve The CSSG Crisis. In *Joint International Conference On Serious Games* (Pp. 117-131). Springer, Cham.

Antonucci, D., 2017. *The Cyber Risk Handbook: Creating And Measuring Effective Cybersecurity Capabilities*. John Wiley & Sons.

Azman, N.D.B.K., Samuel, R. And Osman, I., 2021. social cognitive indicators on mental health of employed young adults in malaysian banking sector. *International Journal Of Accounting*, *6*(33), Pp.46-51.

Balaji, K., 2019. *User Traffic Characteristics Study And Network Security Implications In PWLAN*. Mcgill University (Canada).

Bandura, A. And Walters, R.H., 1977. *Social Learning Theory* (Vol. 1). Prentice Hall: Englewood Cliffs.

Baxter, G. And Sommerville, I., 2011. Socio-Technical Systems: From Design Methods To Systems Engineering. *Interacting With Computers*, *23*(1), Pp.4-17.

Beno, M. And Hvorecky, J., 2021. Data On An Austrian Company's Productivity In The Pre-Covid-19 Era, During The Lockdown And After Its Easing: To Work Remotely Or Not?. *Frontiers In Communication*, *6*, P.46.

Bonacini, L., Gallo, G. And Scicchitano, S., 2021. Working From Home And Income Inequality: Risks Of A 'New Normal'with COVID-19. *Journal Of Population Economics*, *34*(1), Pp.303-360.

Borkovich, D. J. & Skovira, R. J. 2020. Working From Home: Cybersecurity In The Age Of Covid 19. *Issues In Information Systems***,** 234-246.

Boyson, S., 2014. Cyber Supply Chain Risk Management: Revolutionizing The Strategic Control Of Critical IT Systems. *Technovation*, *34*(7), Pp.342-353.

Brenan, M., 2020. US Workers Discovering Affinity For Remote Work. *Gallup*.

Brotherston, L. And Berlin, A., 2017. *Defensive Security Handbook: Best Practices For Securing Infrastructure*. " O'Reilly Media, Inc.".

Brotherston, L. And Berlin, A., 2017. *Defensive Security Handbook: Best Practices For Securing Infrastructure*. " O'Reilly Media, Inc.".

Bulpett, B., 2020. Safeguarding Against The Insider Threat. *Network Security*, *2020*(6), Pp.14-17.

Buomprisco, G., Ricci, S., Perri, R. And De Sio, S., 2021. Health And Telework: New Challenges After COVID-19 Pandemic. *European Journal Of Environment And Public Health*, *5*(2), P.Em0073.

Burke, S. 2020. Analysis And Perspective For Solution Providers And Technology Integrators.

Calder, A., 2017. *Nine Steps To Success: An ISO 27001 Implementation Overview*. IT Governance Ltd.

Caligiuri, P., De Cieri, H., Minbaeva, D., Verbeke, A. And Zimmermann, A., 2020. International HRM Insights For Navigating The COVID-19 Pandemic: Implications For Future Research And Practice.

Carlton, M., Levy, Y. And Ramim, M., 2019. Mitigating Cyber Attacks Through The Measurement Of Non-IT Professionals' Cybersecurity Skills. *Information & Computer Security*.

Chapman, P. 2020. Are Your IT Staff Ready For The Pandemic-Driven Insider Threat? Network Security. *Elsevier Public Health Emergency Collection,* 4**,** 8-11.

Christensen, C. And Euchner, J., 2020. Managing Disruption: An Interview With Clayton Christensen. *Research-Technology Management*, *63*(3), Pp.49-54.

Ciesla, R., 2020. Creating Extremely Secure Encrypted Systems. In *Encryption For Organizations And Individuals* (Pp. 103-148). Apress, Berkeley, CA.

Craigen, D., Diakun-thibault, N. & PURSE, R. 2014. Defining Cybersecurity. *Technology Innovation Management Review,* 4.

Crossland, G., Ertan, A. & Michaelides, N. 2021. Remote Working and Cyber Security. London: Research Institure For Sociotechnical Cyber Security.

Cuerdo-Vilches, T., Navas-Martín, M.Á. And Oteiza, I., 2021. Working From Home: Is Our Housing Ready?. *International Journal Of Environmental Research And Public Health*, *18*(14), P.7329.

Datta, A., 2007. Resource Based View Of Information Systems: A Critique. *Available At SSRN 1029228*.

Dearing, C.K., 2019. Personal Information As An Attack Vector: Why Privacy Should Be An Operational Dimension Of US National Security. *J. Nat'l Sec. L. & Pol'y*, *10*, P.351.

Dubey, A. D. & Tripathi, S. 2020. Analysing The Sentiments Towards Work-From-Home Experience During Covid-19 Pandemic. *Journal Of Innovation Management,* 8**,** 13-19.

Dwivedi, Y.K., Hughes, D.L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J.S., Gupta, B., Lal, B., Misra, S., Prashant, P. And Raman, R., 2020. Impact Of COVID-19 Pandemic On Information Management Research And Practice: Transforming Education, Work And Life. *International Journal Of Information Management, 55,* P.102211.

Eastman, R., Versace, M. And Webber, A., 2015. Big Data And Predictive Analytics: On The Cybersecurity Front Line. *IDC Whitepaper, February*.

Eckert, C., Earl, C., Lebjioui, S. And Isaksson, O., 2013, July. Components Margins Through The Product Lifecycle. In *IFIP International Conference On Product Lifecycle Management* (Pp. 39-47). Springer, Berlin, Heidelberg.

Eemani, H.R., 2017. Analyzing, Implementing And Monitoring Critical Security Controls: A Case Implemented In J & B Group.

Emery, F.E. And Trist, E.L., 1960. Management Science, Models And Techniques.

Feeney, A.B., Frechette, S. And Srinivasan, V., 2017. Cyber-Physical Systems Engineering For Manufacturing. In *Industrial Internet Of Things* (Pp. 81-110). Springer, Cham.

Felstead, A. And Henseke, G., 2017. Assessing The Growth Of Remote Working And Its Consequences For Effort, Well-Being And Work-Life Balance. *New Technology, Work And Employment*, *32*(3), Pp.195-212.

Filkins, B.L., Kim, J.Y., Roberts, B., Armstrong, W., Miller, M.A., Hultner, M.L., Castillo, A.P., Ducom, J.C., Topol, E.J. And Steinhubl, S.R., 2016. Privacy And Security In The Era Of Digital Health: What Should Translational Researchers Know And Do About It?. *American Journal Of Translational Research*, *8*(3), P.1560.

Frenkel, M.O., Giessing, L., Egger-Lampl, S., Hutter, V., Oudejans, R.R., Kleygrewe, L., Jaspaert, E. And Plessner, H., 2021. The Impact Of The COVID-19 Pandemic On European Police Officers: Stress, Demands, And Coping Resources. *Journal Of Criminal Justice*, *72,* P.101756.

Furnell, S. And Shah, J.N., 2020. Home Working And Cyber Security–An Outbreak Of Unpreparedness?. *Computer Fraud & Security*, *2020*(8), Pp.6-12.

Gallardo, R. & Whitacre, B. 2018. 21st Century Economic Development: Telework And Its Impact On Local Income. *Regional Science Policy & Practice*, 10**,** 103-123.

Garcia-Perez, A., Sallos, M.P. And Tiwasing, P., 2021. Dimensions Of Cybersecurity Performance And Crisis Response In Critical Infrastructure Organisations: An Intellectual Capital Perspective. *Journal Of Intellectual Capital*.

Garson, K. And Adams, C., 2008, March. Security And Privacy System Architecture For An E-Hospital Environment. In *Proceedings Of The 7th Symposium On Identity And Trust On The Internet* (Pp. 122-130).

Georgiadou, A., Mouzakitis, S. And Askounis, D., 2021. Detecting Insider Threat Via A Cyber-Security Culture Framework. *Journal Of Computer Information Systems*, Pp.1-11.

Gërvalla, M., Preniqi, N. And Kopacek, P., 2018. IT Infrastructure Library (ITIL) Framework Approach To IT Governance. *IFAC-Papersonline*, *51*(30), Pp.181-185.

Geuens, M. And De Pelsmacker, P., 2017. Planning And Conducting Experimental Advertising Research And Questionnaire Design. *Journal Of Advertising*, *46*(1), Pp.83-100.

Golder, S.A. And Macy, M.W., 2014. Digital Footprints: Opportunities And Challenges For Online Social Research. *Annual Review Of Sociology*, *40*, Pp.129-152.

Griffin, R.W., Phillips, J.M. And Gully, S.M., 2016. *Organizational Behavior: Managing People And Organizations*. Cengage Learning.

Håkansson, A., 2013. Portal Of Research Methods And Methodologies For Research Projects And Degree Projects. In *The 2013 World Congress In Computer Science, Computer Engineering, And Applied Computing WORLDCOMP 2013; Las Vegas, Nevada, USA, 22-25 July* (Pp. 67-73). CSREA Press USA.

Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K. And Stantchev, V., 2016. A Process Framework For Information Security Management.

Hashimoto, G.T., Rosa, P.F., Lopes Filho, E. And Machado, J.T., 2010, August. A Security Framework To Protect Against Social Networks Services Threats. In *2010 Fifth International Conference On Systems And Networks Communications* (Pp. 189-194). IEEE.

Hinsliff, G., 2020. Office Life Is Not Over–But The Way We Work Must Surely Change. *The Guardian*.

Hong, K.S., Chi, Y.P., Chao, L.R. And Tang, J.H., 2003. An Integrated System Theory Of Information Security Management. *Information Management & Computer Security*.

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M. & Mahmood, S. 2020. Cyber Security Threats And Vulnerabilities: A Systematic Mapping Study. *Arabian Journal For Science And Engineering,* 45**,** 3171-3189.

Hussein, M.R., Rahman, M., Mojumder, M., Hassan, J., Ahmed, S., Isha, S.N., Akter, S., Shams, A.B. And Apu, E.H., 2020. Trust Concerns In Health Apps Collecting Personally Identifiable Information During COVID-19-Like Zoonosis. *Arxiv Preprint Arxiv:2009.07403*.

Iakovakis, G., Xarhoulacos, C.G., Giovas, K. And Gritzalis, D., 2021. Analysis And Classification Of Mitigation Tools Against Cyberattacks In COVID-19 Era. *Security And Communication Networks*, *2021*.

International Labour Organization, 2020. ILO Monitor: COVID-19 And The World Of Work. *Updated Estimates And Analysis. Int Labour Organ*.

Ireland, R.D., Hoskisson, R.E., And Hitt, M.A., 2013. The Management Of Strategy: Concepts And Cases. 8th Ed. Mason, OH: South-Western Cengage Learning.

Ismail, S., Sitnikova, E. And Slay, J., 2014, August. Using Integrated System Theory Approach To Assess Security For SCADA Systems Cyber Security For Critical Infrastructures: A Pilot Study. In *2014 11th International Conference On Fuzzy Systems And Knowledge Discovery (FSKD)* (Pp. 1000-1006). IEEE.

Johnstone, A. C., Wech, B., Jack, E. & Beavers, M. Reigning In The Remote Employee: Applying Social Learning Theory To Explain Information Security Policy Compliance Attitudes. 2010. AMCIS Proceedings. 493.

Kapoor, K., Bigdeli, A.Z., Dwivedi, Y.K., Schroeder, A., Beltagui, A. And Baines, T., 2021. A Socio-Technical View Of Platform Ecosystems: Systematic Review And Research Agenda. *Journal Of Business Research*, *128,* Pp.94-108.

Kemmerer, R. A. Cybersecurity. 25th International Conference On Software Engineering, 2003. 705 - 715.

Khan, N. A., Brohi, S. N. & Zaman, N. 2020. Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. Malaysia: Research Gate.

Kimani, K., Oduol, V. And Langat, K., 2019. Cyber Security Challenges For Iot-Based Smart Grid Networks. *International Journal Of Critical Infrastructure Protection*, *25*, Pp.36-49.

Kossek, E. & Lautsch, B. 2018. Work–Life Flexibility For Whom? Occupational Status And Work–Life Inequality In Upper, Middle, And Lower Level Jobs. *Academy Of Management Annals***,** 5-36.

Kshetri, N. And Kshetri, D.N., 2016. *Quest To Cyber Superiority*. Springer.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. And Bellekens, X., 2021. Cyber Security In The Age Of Covid-19: A Timeline And Analysis Of Cyber-Crime And Cyber-Attacks During The Pandemic. *Computers & Security*, *105*, P.102248.

Kumari, K. And Yadav, S., 2018. Linear Regression Analysis Study. *Journal Of The Practice Of Cardiovascular Sciences*, *4*(1), P.33.

Langner, R., 2013. To Kill A Centrifuge. A Technical Analysis Of What Stuxnet's Creators Tried To Achieve The Langner Group. *The Langner Group, Tech. Rep.*

Lavie, D., 2006. The Competitive Advantage Of Interconnected Firms: An Extension Of The Resource-Based View. *Academy Of Management Review*, *31*(3), Pp.638-658.

Leuprecht, C., Skillicorn, D.B. And Tait, V.E., 2016. Beyond The Castle Model Of Cyber-Risk And Cyber-Security. *Government Information Quarterly*, *33*(2), Pp.250-257.

Lin, H. And Bergmann, N.W., 2016. Iot Privacy And Security Challenges For Smart Home Environments. *Information*, *7*(3), P.44.

Liu, C., Alrowaili, Y., Saxena, N. And Konstantinou, C., 2021. Cyber Risks To Critical Smart Grid Assets Of Industrial Control Systems. *Energies*, *14*(17), P.5501.

Lykou, G., Anagnostopoulou, A., Stergiopoulos, G. And Gritzalis, D., 2018, September. Cybersecurity Self-Assessment Tools: Evaluating The Importance For Securing Industrial Control Systems In Critical Infrastructures. In *International Conference On Critical Information Infrastructures Security* (Pp. 129-142). Springer, Cham.

Macintyre, C.R., Engells, T.E., Scotch, M., Heslop, D.J., Gumel, A.B., Poste, G., Chen, X., Herche, W., Steinhöfel, K., Lim, S. And Broom, A., 2018. Converging And Emerging Threats To Health Security. *Environment Systems And Decisions*, *38*(2), Pp.198-207.

Maennel, K., Mäses, S. And Maennel, O., 2018, November. Cyber Hygiene: The Big Picture. In *Nordic Conference On Secure IT Systems* (Pp. 291-305). Springer, Cham.

Malecki, F., 2020. Overcoming The Security Risks Of Remote Working. *Computer Fraud & Security*, *2020*(7), Pp.10-12.

Mandl, I. And Biletta, I., 2018. Overview Of New Forms Of Employment-2018 Update.

Ma, X., 2022. IS Professionals' Information Security Behaviors In Chinese IT Organizations For Information Security Protection. *Information Processing & Management*, *59*(1), P.102744.

Mcilwraith, A., 2021. *Information Security And Employee Behaviour: How To Reduce Risk Through Employee Education, Training And Awareness*. Routledge.

Moore, T., 2010. The Economics Of Cybersecurity: Principles And Policy Options. *International Journal Of Critical Infrastructure Protection*, *3*(3-4), Pp.103-117.

Mihailović, A., Cerović Smolović, J., Radević, I., Rašović, N. And Martinović, N., 2021. COVID-19 And Beyond: Employee Perceptions Of The Efficiency Of Teleworking And Its Cybersecurity Implications. *Sustainability*, *13*(12), P.6750.

Mohsin, K. 2020. Cybersecurity In Corona Virus (COVID-19) Age. *SSN*.

Mudrinich, E.M., 2012. Cyber 3.0: The Department Of Defense Strategy For Operating In Cyberspace And The Attribution Problem. *AFL Rev.*, *68*, P.167.

Nelson, R.R. And Romer, P.M., 1996. Science, Economic Growth, And Public Policy. *Challenge*, *39*(1), Pp.9-21.

Okereafor, K. & Manny, P. 2020. Understanding Cybersecurity Challenges Of Telecommuting And Video Conferencing Applications In The COVID-19 Pandemic. *Journal Homepage:* ***Http://Ijmr****. Net. In,* 8.

Okes, D., 2019. *Root Cause Analysis: The Core Of Problem Solving And Corrective Action*. Quality Press.

Okuku, A., Renaud, K., & Valeriano, B. (2015). Cybersecurity Strategy's Role In Raising Kenyan Awareness Of Mobile Security Threats. Information & Security, 32(2), 1.

Ong, S.F., 2012. Constructing A Survey Questionnaire To Collect Data On Service Quality Of Business Academics.

Organisation For Economic Co-Operation And Development, 2020. *Productivity Gains From Teleworking In The Post COVID-19 Era: How Can Public Policies Make It Happen?*. OECD Publishing.

Ozcelik, H., Langton, N. And Aldrich, H., 2008. Doing Well And Doing Good: The Relationship Between Leadership Practices That Facilitate A Positive Emotional Climate And Organizational Performance. *Journal Of Managerial Psychology*.

Ozimek, A. 2020. The Future Of Remote Work. *SSRN*.

Parker, L.D., 2020. The COVID-19 Office In Transition: Cost, Efficiency And The Social Responsibility Business Case. *Accounting, Auditing & Accountability Journal*.

Pasmore, W., Winby, S., Mohrman, S.A. And Vanasse, R., 2019. Reflections: Sociotechnical Systems Design And Organization Change. *Journal Of Change Management*, *19*(2), Pp.67-85.

Pearce, J.A. And Robinson Jr, R.B., 2008. Strategic Management; Formulation: Formulation, Implementation And Control. New York, NY: Mcgraw-Hill

Pfleeger, C.P. And Pfleeger, S.L., 2012. *Analyzing Computer Security: A Threat/Vulnerability/Countermeasure Approach*. Prentice Hall Professional.

Plėta, T., Tvaronavičienė, M. And Della Casa, S., 2020. Cyber Effect And Security Management Aspects In Critical Energy Infrastructures. *Insights Into Regional Development*.

Pranggono, B. & Arabo, A. 2021. COVID-19 Pandemic Cybersecurity Issues. *Internet Technology Letters,* 4**,** E247.

Reed, E., Khoshnood, K., Blankenship, K.M. And Fisher, C.B., 2014. Confidentiality, Privacy, And Respect: Experiences Of Female Sex Workers Participating In HIV Research In Andhra Pradesh, India. *Journal Of Empirical Research On Human Research Ethics*, *9*(1), Pp.19-28.

Rhee, H.S., Kim, C. And Ryu, Y.U., 2009. Self-Efficacy In Information Security: Its Influence On End Users' Information Security Practice Behavior. *Computers & Security*, *28*(8), Pp.816-826.

Richardson, J. And Kelliher, C., 2015. Managing Visibility For Career Sustainability: A Study Of Remote Workers. In *Handbook Of Research On Sustainable Careers*. Edward Elgar Publishing.

Robertson, J. And Riley, M., 2018. The Big Hack: How China Used A Tiny Chip To Infiltrate Us Companies. *Bloomberg Businessweek*, *4*(2018).

Rumelt, R.P., 1984. Towards A Strategic Theory Of The Firm. *Competitive Strategic Management*, *26*(3), Pp.556-570.

Saleem, M., 2019, June. Brexit Impact On Cyber Security Of United Kingdom. In *2019 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)* (Pp. 1-6). IEEE.

Savić, D. 2020. COVID-19 And Work From Home: Digital Transformation Of The Workforce. *The Grey Journal***,** 101-103.

Serianu 2020. Kenya Cybersecurity Report 2020. Nairobi.

Setia, P., Setia, P., Venkatesh, V. And Joglekar, S., 2013. Leveraging Digital Technologies: How Information Quality Leads To Localized Capabilities And Customer Service Performance. *MIS Quarterly*, Pp.565-590.

Singer, P.W. And Friedman, A., 2014. *Cybersecurity: What Everyone Needs To Know*. Oup Usa.

Sittig, D.F., Belmont, E. And Singh, H., 2018, March. Improving The Safety Of Health Information Technology Requires Shared Responsibility: It Is Time We All Step Up. In *Healthcare* (Vol. 6, No. 1, Pp. 7-12). Elsevier.

Sharma, A., Adhikary, A. And Borah, S.B., 2020. Covid-19′ S Impact On Supply Chain Decisions: Strategic Insights From NASDAQ 100 Firms Using Twitter Data. *Journal Of Business Research, 117*, Pp.443-449.

Škiljić, A. 2020. Cybersecurity And Remote Working: Croatia's (Non-) Response To Increased Cyber Threats. *International Cybersecurity Law Review*, 1**,** 51-61.

Skopik, F., Settanni, G. And Fiedler, R., 2016. A Problem Shared Is A Problem Halved: A Survey On The Dimensions Of Collective Cyber Defense Through Security Information Sharing. *Computers & Security*, *60,* Pp.154-176.

Socha, S., 2021. *An Exploration Of Factors Influencing Female Career Progression In The United States* (Doctoral Dissertation, The College Of St. Scholastica).

Sovacool, B.K. And Hess, D.J., 2017. Ordering Theories: Typologies And Conceptual Frameworks For Sociotechnical Change. *Social Studies Of Science*, *47*(5), Pp.703-750.

Srinivas, J., Das, A.K. And Kumar, N., 2019. Government Regulations In Cyber Security: Framework, Standards And Recommendations. *Future Generation Computer Systems*, *92*, Pp.178-188.

Stephens, J. And Valverde, R., 2013. Security Of E-Procurement Transactions In Supply Chain Reengineering. *Computer And Information Science*, *6*(3).

Teece, D.J., 2007. Explicating Dynamic Capabilities: The Nature And Microfoundations Of (Sustainable) Enterprise Performance. *Strategic Management Journal*, *28*(13), Pp.1319-1350.

Thompson, E.C., 2017. The Cybersecurity Road Map. In *Building A HIPAA-Compliant Cybersecurity Program* (Pp. 149-167). Apress, Berkeley, CA.

Varshney, K.R. And Alemzadeh, H., 2017. On The Safety Of Machine Learning: Cyber-Physical Systems, Decision Sciences, And Data Products. *Big Data*, *5*(3), Pp.246-255.

Wan, X., Wang, W., Liu, J. And Tong, T., 2014. Estimating The Sample Mean And Standard Deviation From The Sample Size, Median, Range And/Or Interquartile Range. *BMC Medical Research Methodology*, *14*(1), Pp.1-13.

Wanyonyi, V., 2020. *Information Security Management Toolkit For ISO/IEC 27001 Standard, Case Of Small-To-Medium Sized Enterprises (Smes)* (Doctoral Dissertation, University Of Nairobi).

Webster, M., 2021. *Do No Harm: Protecting Connected Medical Devices, Healthcare, And Data From Hackers And Adversarial Nation States*. John Wiley & Sons.

Weil, T. And Murugesan, S., 2020. IT Risk And Resilience—Cybersecurity Response To COVID-19. *IT Professional*, *22*(3), Pp.4-10.

Wernerfelt, B., 1984. A Resource‐Based View Of The Firm. *Strategic Management Journal*, *5*(2), Pp.171-180.

Westerman, G. And Hunter, R., 2007. IT Risk. *George Westerman And Gartner, Boston*.

Wheeler, T., 2018. In Cyberwar, There Are No Rules. *Foreign Policy*, *12*, Pp.3-4.

Williams, C. M., Chaturvedi, R. & Chakravarthy, K. 2020. Cybersecurity Risks In A Pandemic. *Journal Of Medical Internet Research,* 22**,** E23692.

Wirth, A. 2020. Cyberinsights: COVID-19 And What It Means For Cybersecurity. *Biomedical Instrumentation & Technology,* 54**,** 216-219.

APPENDIX 1

QUESTIONNAIRE

MODEL ON MITIGATING CYBERSECURITY CHALLENGES FOR SECURE REMOTE WORKING DURING COVID-19 AND BEYOND: A CASE STUDY OF FINANCIAL REGULATORY STATE CORPORATIONS IN KENYA

This research is purely for academic purposes only. Please answer the questions as precisely and honestly as possible. Information provided will kept confidential.

SECTION A: DEMOGRAPHIC CHARACTERISTICS

What is the name of your Organization?

[ ] Capital Markets Authority

[ ] Insurance Regulatory Authority

[ ] Retirements Benefits Authority

Which department do you work in?

[ ] ICT

[ ] FINANCE

[ ] MARKET CONDUCT/OPERATIONS

What is your highest level of education?

[ ] Diploma

[ ] Undergraduate

[ ] Post-graduate

SECTION B: REMOTE WORKING

1. **At the onset of Covid-19, did your organization adopt remote working or working from home?**
   [ ] YES
   [ ] NO
2. **Were you facilitated with the requisite computing tools e.g. laptop, to enable you to work remotely?**
   [ ] YES
   [ ] NO
3. **If your answer is [NO] above, does your organization allow you to use you own device to work from home?**
   [ ] YES
   [ ] NO
4. **Does your organization assess your computing device (personally owned or provided by your organization) to determine the security configurations and compliance level to security policies in place for remote working?**

[ ] YES
[ ] NO
[ ] To Some extent

5. **When working from home, are you able to access all ICT resources required to do your work as though you were physically present at the office?**
   [ ] YES
   [ ] NO
   [ ] Only some resources
6. **Do you have administrative privileges on your machines?**
   [ ] YES
   [ ] NO
   [ ] I Don't know
7. **Are you able to alter or disable security systems installed on your provided computing tool when working remotely?**
   [ ] YES
   [ ] NO
8. **Are you able to download and install software or alter the system configurations on your computing device when working remotely?**
   [ ] YES
   [ ] NO
9. **Do you use your computing device for personal use while working remotely?**
   [ ] YES
   [ ] NO
10. **Do you allow your family members to use your computing device when working remotely/working from home?**
    [ ] YES
    [ ] NO

SECTION C: ORGANIZATION CYBERSECURITY PREPAREDNESS IN FACILITATING SECURE REMOTE WORKING

1. **Is there a standard documented process for on-boarding employees and providing access to ICT resources remotely?**
   [ ] YES
   [ ] NO
2. **How frequent does your organization update staff on cybersecurity threats and vulnerabilities during remote working?**
   [ ] Very Frequently
   [ ] Frequently
   [ ] Occasionally
   [ ] Rarely
   [ ] Never
3. **What is the level of cybersecurity awareness and sensitization in your organization?**
   [ ] Very Hign
   [ ] High
   [ ] Medium
   [ ] Low
   [ ] Very Low

To what extent do you agree with the following statements on a scale of 1 - 5 where 1 means "strongly disagree" and 5 means "strongly agree".

4. **The organization conducts a rigorous cybersecurity awareness and sensitization exercise during remote working.**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

5. **Remote employees differ from office employees in their perceived levels of security, self-efficacy and compliance with relevant policies and practices**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

6. **Your organization is finding it harder to administer cybersecurity measures during remote working**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

7. **Human error poses the greatest cybersecurity threat to the organization.**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

8. **Our organization does not have adequate cybersecurity framework, policy or procedures for remote workers**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

9. **Our organization has the capability to monitor remote user activity for cybersecurity threats**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

10. **Management has instituted measures to respond to cybersecurity threats during remote working**
    [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

SECTION D: CYBERSECURITY THREATS

1. **Have cybersecurity attacks been more frequent during remote working in the Covid-19 period?**
   [ ] YES
   [ ] NO
2. Have cyber-attacks have become more sophisticated and dangerous in terms of negative consequences
   [ ] YES
   [ ] NO

On a scale of 1 - 5 where 1 means "Very frequently" and 5 means "Never":

3. What is the frequency of attacks during the remotely working period?

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

4. What threats has your organization encountered during the remote working period? (Select all that apply)
   [ ] Increased social engineering attacks
   [ ] Phishing (email) campaigns and scams
   [ ] Ransonmware
   [ ] Malware and Viruses
   [ ] Password attacks
   [ ] Remote access exploitation
   [ ] Other…………………………………….

5. In your opinion, what has accelerated the above attacks during remote working? (select all that apply)
   [ ] Lack of employee cybersecurity awareness and sensitization
   [ ] Unsecured remote connections

[ ] Use of unsecured network (WIFI/LAN) connections when working remotely
[ ] Relaxed or reduced levels of employee security and compliance when working remotely
[ ] Lack of critical and security updates and patches on computing devices when working remotely
[ ] Loss of connectivity to central ICT Servers
[ ] Sharing of computing devices (laptops) with others people while working from home
[ ] Sharing of passwords
[ ] Other………………………

6. What are the challenges that have made it difficult for your organization to mitigate cybersecurity attacks? (Select all that apply)
[ ] Use of weak passwords
[ ] Lack of ICT Technical Capacity
[ ] Lack of adequate security protection measures and tools
[ ] Network, System and Application vulnerabilities
[ ] Inability to detect and respond to cybersecurity attacks
[ ] Lack of adequate financial resources
7. What impact has the cybersecurity threats had on your organization? (select all that apply)
[ ] Data Loss
[ ] Data corruption
[ ] Unavailability of critical ICT services
[ ] Privacy Breach
[ ] Other…..

To what what extent do you agree with the statements below on a scale of 1 - 5 where 1 means 'Strongly disagree' and 5 means 'Strongly agree'.

8. Our organization is finding it harder to administer cyber security measures during remote working in the Covid 19 period

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5
9. Our organization has lost or has reduced visibility on the breaches and attacks staff working from home are facing

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

10. Organizations are investing heavily in external security at the expense of internal security, leading to insider threats and attacks

    [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

SECTION E: CYBERSECURITY MANAGEMENT PRACTICES

1. **Is your organization able to monitor and control user/staff activity when they are working remotely?**
[ ] YES
[ ] NO
2. **Is your organization able to monitor and control remote access connections from employees working remotely?**
[ ] YES
[ ] NO
3. **Has your organization implemented any measures to detect, prevent and respond to cybersecurity threats encountered by staff as they work from home?**
[ ] YES

[ ] NO

4. **What cybersecurity measures has your organization put in place to ensure secure remote working? (select all that apply)**
   [ ] Enterprise End-Point Anti-Virus
   [ ] Firewall
   [ ] Email Spam filtering
   [ ] Identity and Access Management
   [ ] Web Application Firewall
   [ ] Remote Access VPN
5. On a scale of 1 – 5 (where one means “extremely effective” and 5 means “not effective”, how effective are the cybersecurity measures implemented in your organization in detecting, protecting and responding to threats.

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5
6. On a scale of 1 – 5 (where one means “very high” and 5 means “very low”, what is the level of user device protection controls implemented to mitigate cybersecurity threats for secure remote working?

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5
7. On a scale of 1 - 5 where 1 means 'Strongly disagree' and 5 means 'Strongly agree' User computing devices are constantly updated with latest patches, anti-malware tools, and security configurations.

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5
8. How often does the organization conduct vulnerability assessment and penetration testing (VAPT)?

   [ ] Monthly [ ] Quarterly [ ] Bi-Annually [ ] Annually [ ] Never
9. **Has your organization implemented identity and access management system such as Multi-Factor authentication for secure remote access?**
   [ ] YES
   [ ] NO

SECTION F: IMPLEMENTED CYBERSECURITY MODELS

1. **Has your organization adopted any framework, model or other methodology to enhance its cybersecurity posture?**
   [ ] YES
   [ ] NO
2. **If Yes, which framework or standard has your organization adopted? (Select all that apply)**
   [ ] NIST
   [ ] ISO/IEC 27001:2013/2015 (ISMS)
   [ ] COBIT
   [ ] ITIL
   [ ] CIS Controls
3. **What is the extent of implementation of the adopted framework or standard?**
   [ ] Full Implementation
   [ ] Partial Implementation
   [ ] Initial Implementation
   [ ] No Implementation
4. On a scale of 1 - 5 where 1 means 'Strongly disagree' and 5 means 'Strongly agree', t**he adoption of the framework or standard has improved the cybersecurity posture of the organization with regard to remote working.**

   [ ] 1 [ ] 2 [ ] 3 [ ] 4 [ ] 5

5. **Does your organization have a comprehensive cybersecurity risk management framework**
   [ ] YES
   [ ] NO
6. **Does your organization conduct a cybersecurity risk assessment?**
   [ ] YES
   [ ] NO
7. **Does your organization have an Cybersecurity Incident Management or Incident response plan?**
   [ ] YES
   [ ] NO
8. **Does your organization have an accountable person or committee responsible for cybersecurity function?**
   [ ] YES
   [ ] NO
9. **Does Senior Management, Executive or Board have visibility of cybersecurity issues impacting the organization?**
   [ ] YES
   [ ] NO

THANK YOU FOR YOUR TIME