2024

Factors influencing the adoption of cybersecurity in large manufacturing companies in Nairobi County.

Ngunju, Sharon
Strathmore Business School
Strathmore University

FACTORS INFLUENCING THE ADOPTION OF CYBERSECURITY IN LARGE MANUFACTURING COMPANIES IN NAIROBI COUNTY

SHARON NGUNJU

ADMISSION NO. 076574

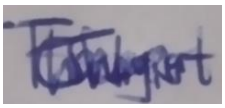
THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF COMMERCE, SCHOOL OF BUSINESS, STRATHMORE UNIVERSITY

DECEMBER, 2023

DECLARATION

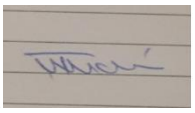
I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Sharon Ngunju

Signature…  Date: 02 December 2023

This thesis has been reviewed and submitted for examination with my approval as Strathmore University supervisor

Dr. Tabitha Waithaka (Supervisor)
Lecturer
Strathmore University Business School

Signature…  Date: 02 December 2023

Dr. Ceasar Mwangi
Executive Dean
Strathmore University Business School.

Dr. Bernard Shibwabo
Director, Office of Graduate Studies

ABSTRACT

Cyberthreats are now universal and affect most organizations around the world. This therefore makes it critical for organizations to adopt cybersecurity measures. This study evaluated how technological factors, organizational resource factors and management factors influence the adoption of cybersecurity in large manufacturing companies in Nairobi County. The research was guided by the Human, Organization and Technology theory and General Deterrence theory. The study focused on 114 large manufacturing firms who are members of Kenya Association of Manufacturers (KAM, 2021). The respondents for the survey were either the Chief Technology Officers/Chief Information Security Officers/Information Technology Managers and ICT Officer/Systems Analyst/System Administrators. The total sample size of the respondents was therefore 228. A structured research questionnaire was adopted in the survey. The data collection for the study was done using Google forms and physical data collection where plausible. The study obtained 80.7% response rate and the collected research data was coded into SPSS. Data was analyzed using descriptive measures, correlation, and regression analysis. The research showed a positive relationship between the organizational resource factors, management factors, and technological factors with adoption of cybersecurity in manufacturing companies in Nairobi County. The results of the regression analysis showed that 41.7% variation in the adoption of cybersecurity could be determined by their organizational resources, management capabilities and technological capability. Hence, the overall regression established that the selected factors contribute significantly to the adoption of cybersecurity. The study recommends that to adopt cybersecurity, the firms need to be ready to allocate significant resources, both financial, and technological to ensure that they meet the high costs associated with pursuing adoption of cybersecurity. The study also recommends that managers align security decisions with organizational goals and capabilities to reduce organizational misalignment which can affect adoption of cybersecurity.

Keywords: cybersecurity, organizational resource factors, management factors, technological factors, manufacturing industry

ACKNOWLEDGEMENT

I thank God for enabling me to complete my studies. I am grateful to my family Jane, Eric and Jesse for the support. Special thanks to my supervisor, Dr. Tabitha Waithaka for her prompt response to my work and for the invaluable support and guidance throughout the research process. May the Lord bless you and keep you all.

DEDICATION

I dedicate this work to God and my family Jane, Eric and Jesse.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

CA: Communication Authority of Kenya

CERT: Computer Emergency Response Team

CIO: Chief Information Officer

CISO: Chief Information Security Officer

GCI: Global Cybersecurity Index

GDPR: General Data Protection Regulation

HOT: Human, Organization and Technology Theory

ICT: Information and Communications Technology

IMF: International Monetary Fund

IR: Incident Response

IRM: Institute of Risk Management

IS: Information Systems

ITU: International Telecommunication Union

KAM: Kenya Association of Manufacturers

KNBS: Kenya National Bureau of Statistics

NIST: National Institute of Standards and Technology

SME: Small and Medium Enterprises

WEF: World Economic Forum

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

The manufacturing sector has gone through several revolutions (Mullet et al., 2021). Mechanization was the first stage (Mullet et al., 2021). Then came mass production and electricity in the second stage (Mullet et al., 2021). The third one occurred in the 1970s with the introduction of automation and IT equipment bringing digital technologies into factories (Mullet et al., 2021). New features such as remote access to networks and devices has appeared, thus making possible a wide range of cyberattacks (Aman & Shukaili, 2021). Moreover, these systems are now available over the internet (Pavel, 2021). Specific impacts to manufacturing production systems could emerge in varying forms which include, disruption to normal operations, equipment and asset damage, delayed or lost productions, products launch, loss of customer trust, loss of brand value, diminishing competitive advantage, loss of revenue and loss or injury to human life (Ani et al., 2017). The most common types of cyber-attacks in the manufacturing industry include denial of service attacks, theft of secrets and sabotage of critical infrastructure and machines (Mullet et al., 2021).

Cybersecurity can be defined as the protection of cyber space, electronic information, Information Communication Technologies that facilitate cyber space and the users of cyber space that are vulnerable to attacks originating in cyberspace (Kortjan & Von Solms, 2014). The goal of cybersecurity is to reduce risk and mitigate the potential risks associated with cyber-attacks (Von Solms & Van Niekerk, 2013). According to researchers, cybersecurity measures are not only an expense, but an opportunity for value creation (Kennison & Chan-Tin, 2020). As a result, in determining issues such as starting a new business or entering new markets, new research and development, mergers and acquisitions, new technology adoption and investment in large scale facilities, cybersecurity should be considered (Aman & Shukaili, 2021).

Cyber-crime is one of the biggest barriers to the adoption of digital transformation strategies as it is responsible for exploiting the weaknesses of systems as well as human related weaknesses (Linkov & Palma-Oliveira, 2017). Globally, cyber-crime has cost the economy between $300 billion and $1 trillion, or 0.4 to 1.4 percent of the global Gross Domestic Product [GDP] (Farahbod et al., 2020). Recent global events include the 2019 attack on Cebuana Lhuillier, which affected 900,000 customers of the Philippines-based organization (Merez, 2019) and the 2018 attack on SingHealth, which compromised the personal health information of 1.5 million Singaporean patients (Vincent, 2018). Tesco was the target of a cyber-attack in October 2021, and as a result, customers were unable to place orders through the company's website and app and Tesco was forced to use a virtual waiting room to manage demand (Justin et al., 2023). As a result, cyber-

attacks cost the United Stated manufacturing sector nearly $240 billion in revenue and 42,220 manufacturing jobs between 2002 and 2012 (Lykou et al., 2019). The World Economic Forum reported that cyberattacks had increased by 50,1% due to the pandemic (WEF, 2020).

The Cybersecurity Exposure Index (CEI), which regularly surveys 108 countries on all continents worldwide listed the countries that are least and most affected by cybercrime. In terms of cybersecurity threats, Africa was the most affected continent while Europe is the least exposed to cybersecurity threats (CEI, 2020). Finland, Denmark, Luxembourg, Australia, and Estonia were the countries that were least exposed to cybercrime while African countries were highly vulnerable to cybercrime as there is no single country on this continent that appears on the list of the world's most minor cybersecurity-exposed countries (CEI, 2020). In Africa, Ethiopia was the country that experiences the highest threat to cybersecurity followed by Tanzania, Zimbabwe, Algeria, and Cameroon (CEI, 2020). According to the Africa Tech (2020), most developing countries considered cybersecurity necessary but they could not invest adequate funds due to pressing needs such as crime prevention, food deprivation, inequality, unemployment, and a lack of skilled labor.

Cybersecurity breaches have cost organizations billions of dollars annually due to lost sales, fines, and settlement costs (Deloitte, 2019). Additionally, indirect costs associated with reputational damage and customer flight may lead organizations to lose market share in the longer term. Unsurprisingly, data breaches represent IT leaders' biggest concern (Alawida et al., 2022). Regulatory and policy frameworks can be essential for shaping cybersecurity practices and raising people's awareness of cybersecurity. Further efforts by the Government of Kenya (GOK, 2021) saw the introduction of the National Cybersecurity Strategy to provide a secure online environment to conduct business, accompanied by the rolling out of 4G internet coverage by telecommunication providers.

Moreover, Kenya launched the Cybersecurity and Protection Bill in 2016 to provide increased security in cyberspace, enabling greater information sharing and national security (Banga & Willem, 2018). The government has also taken steps to implement the National Cyber security Strategy 2022 and upgrade institutions such as the Kenya Computer Incident Response Team (KE-CIRT) and establish the National Cyber security Centre of Excellence (NCCoE) to enhance its cybersecurity capacity. However, according to Kabanda et al. (2018) there is little research on cybersecurity issues in African countries hence the need for the current study to establish factors influencing adoption of cybersecurity specifically on the large manufacturing sector within the Kenyan context.

1.1.1 Factors Influencing the Adoption of Cybersecurity

Adopting a particular technology to support various organizational functions is often affected by the rate of technological change and the general acceptance by the technology users (Georgiadou et al., 2022). To this end, several theories and models have sought to explain the users' acceptance of new technologies and their intentions of use. These theories pointed out the factors leading organizations to adopt technologies in pragmatic terms (Muthu et al., 2016).

Rogers (1995) proposed the theory of Diffusion of Innovations (DOI) which established the foundation of research on innovation acceptance and adoption among individuals and organizations. This theory explained that innovations and adoption happen after going through several stages, including understanding, persuasion, decision making, implementation, and confirmation that results in an adoption curve of innovations wherein lie the innovators, early adopters, early majority, late majority, and laggards (Rogers, 1995). Another model is the task-technology fit model which assumes that a good fit between the task to be accomplished and the technology aims at increasing performance and effectiveness (Goodhue & Thompson, 1995). Fishbein and Ajzen (1975) also proposed a broad Theory of Reasoned Action that focused on subjective state of individuals making adoption decisions. The researchers concluded that attitude and beliefs about technology influence the user behavior (Fishbein and Ajzen, 1975). To increase the explanatory power of the Theory of Reasoned Action, Ajzen (1991) added perceived control of behavior as a major factor that users perceive may limit their behavior. This resulted in an expanded theory called the Theory of Planned Behavior (Ajzen, 1991).

Finally, one of the most widely studied model in technology acceptance is the Technology Acceptance Model (TAM) which focused on psychological factors namely perceived usefulness to both self and the organization, and the perceived ease of use of a particular technology (Davis et al., 1989). The perceived usefulness is the potential users' subjective likelihood that using a specific system will improve their action. On the other hand, perceived ease of use is the degree to which the potential users expect the target system to be effective (Davis et al., 1989). Notably, usefulness and ease of use are considered among the most powerful factors in adoption decisions (Davis, 2003). This study was related to the General Deterrence theory which established a theoretical foundation to discuss adoption of cybersecurity.

The emphasis of most academic work in the early years of cyber research was on the technological aspects of cybersecurity (Kayode et al., 2016; Senarak, 2021; Gao et al., 2023). However, researchers have concluded that the cyberspace cannot rely solely on technology features in the decades since 2000. Instead, it is

influenced by people and processes, in addition to technology (Prasetio & Nurliyana, 2023). Similar studies revealed that the greatest risks to cybersecurity in organizations arise from non-technological factors and human resources. In a successful cybersecure organization, all technical, organizational, procedural and human issues need consideration to adapt to the changing environment and recover from cyberattacks (Zaqueu & Mawela, 2023;Linkov & Palma-Oliveira, 2017). Management support, organizational resources, processes and technology were also identified as four factors in cybersecurity implementation (Barth et al., 2022). Mutunhu et al. (2022) stated that to fully study the impact of all the main factors affecting cybersecurity and the importance of each factor, a comprehensive framework that combined these factors was needed. It was also confirmed by Bada et al. (2014) that to understand the various factors that can influence cybersecurity from various perspectives, it is not enough to consider only one aspect, but a more comprehensive model is needed that combines the factors that can influence cybersecurity adoption (Dupont, 2019).

Studies on factors influencing cybersecurity adoption have been carried out in different contexts and have diverse focus. For example, in Bhutan, Choejey et al., (2016) study on the critical success factors for cybersecurity implementation in government organizations, found that successful cybersecurity implementation is dependent on a thorough understanding of cyber threats and challenges to organizational information assets. It also depended on the identification of responsible, dedicated personnel to lead and direct cybersecurity initiatives, as well as on awareness and training, policy and standards, adequate funding and budgetary commitment to cybersecurity projects.

In Nigeria, Rufai et al. (2020) analyzed the factors influencing SMEs cybersecurity implementations whereby, SMEs recognized a lack of relevant skills and financial resources to address cybersecurity concerns. Kabanda et al. (2018) found that SME's perception of cybersecurity was influenced by internal factors such as budget, top management support and perceived ease of use. In South Africa, the study by Kent et al. (2016) sought to understand factors influencing the implementation of cybersecurity controls in SMEs in South Africa. According to the study, the main factors influencing the implementation of cybersecurity controls were a lack of management support due to other company objectives, a low budget and a lack of resources with technical skills and cybers security tools. The use of the of the above factors is also based on several theories including institutional theory (Choejey et al., 2016; Armenia et al., 2021), prevention theory (Kent et al., 2016) and macro ergonomics theory (Kabanda et al., 2018) which includes internal organizational factors. The term organizational factor is used in a study by Bagheri (2020) to refer to a variety of organizational factors that influence the workplace, such as organizational structure, policies,

social relationships and communication, decision-making process, employees' knowledge and skills, cultural issues, and other elements.

In Kenya, Mose (2019) investigated cybersecurity readiness among Kenyan deposit taking savings and credit cooperatives, which found that cybersecurity policies, technical and logistical security competencies, and top management support were the most important factors, whereas Kiganda (2022) evaluated cyber resilience in Kenyan microfinance institutions and found that management factors, resource factors and regulatory factors were the main factors. Chizanga et al. (2022) study showed that cybersecurity awareness, cultural issues, cybersecurity training, infrastructure and policies for ICT cybersecurity practices were the main factors determining cybersecurity readiness in public universities in Kenya. Kaibiru et al. (2023) study sought to determine the status of cybersecurity skill gap in higher education in Kenya. The study found that lack of skilled manpower was one of the main pain points in addressing cybersecurity adoption. Otieno (2018) study found that the challenges of cybersecurity in Kenyan organizations centered around adequate manpower or personnel, cost and infrastructure required to ensure information systems are well secured. Muhati (2018) study explored cyber resilience in SMEs considering leadership factors and government cyber policies as the main factors.

As shown by evidence from the various studies reviewed in various contexts, the factors influencing adoption of cybersecurity can be classified as technological factors, management factors and organizational resource factors. These factors were the focus of the current study since they are critical in ensuring effective adoption of cybersecurity measures**.**

1.1.2 Adoption of Cybersecurity

According to Bloomberg (2020), over 60% of manufacturing companies use technical cybersecurity counter measures such as antivirus software, firewalls, anti-spyware software, virtual private networks (VPNs), vulnerability, patch management, data encryption in transit, and intrusion detection systems. Mullet et al. (2021) argue that to ensure the effectiveness of security measures and to maintain security policies, manufacturing companies should employ multiple cybersecurity strategies. Some researchers have argued that adoption of cybersecurity is explained by failure and recovery time (Rawindaran et al., 2021; Shojaifar, 2020). However, other researchers adopted a broader perspective believing that adoption of cybersecurity encompass more than recovery. Glory et al. (2017) stated that cybersecurity has four goals. These include anticipation, withstanding, recovery and evolving.

Research efforts have been made to develop organizational evaluation tools for cybersecurity. For instance, Mijwil (2023) proposed the cybersecurity recovery model incorporated the recovery life cycle of preparation, detection, recovery and post-incident analysis. Bagheri (2020) conducted an investigation of the factors that influence information systems security in SMEs focused on planning and decision-making procedures. The study developed a conceptual model for information system security in SMEs consisting of external and internal enablers. The external enablers were, having a business continuity and recovery plan. Kennison & Chan-Tin (2020) proposed a cybersecurity checklist with a series of questions for self-assessment. In 2016, Gisladottir et al. (2016) calculated cybersecurity system by applying a different approach to those used in the studies discussed above. This study focused on the absorption and recovery phases of cybersecurity with an emphasis on organizational regulations.

Another cybersecurity study focused on the recovery stage of cybersecurity, proposing a framework of the main steps required for recovery during cyber-attack (Chowdhury et al., 2022). Those steps were regular maintenance work (to handle typical issues and reduce known threats), supporting activities (to strengthen the response) and the emergency response and recovery plan (to deal with known and unknown threats) (Chowdhury et al., 2022). The importance of the recovery processes in cybersecurity was also emphasized by Okereafor (2020), who examined other cybersecurity operational issues, namely asset categorization, risk management, emergency response activities and learning from the past experience.

Lykou et al. (2019) conducted research to identify cybersecurity best practices for smart airport systems. For organizational cybersecurity practices in an airport environment, approaches identified were access management, security of third-party providers, user cybersecurity awareness training and security response planning. Another evaluation tool, was the cyber value at risk developed by the World Economic Forum (2019), aimed to quantify cyber risks. The cyber value at risk calculated the total loss value of a cyber-attack. It identified the potential cyber risks in an organization and contributed to evaluating the level of cybersecurity (World Economic Forum, 2019). The component of the model included vulnerability (existence of vulnerability, security maturity model and number of failures), assets (tangible and intangible) and information on attackers (attacker classification, attack classification and motivation).

The Cyber Resilience Review assessment tool was designed by CERT Division of the Software Engineering Institute at Carnegie Mellon University in 2013. The Cyber Resilience Review is a questionnaire composed of 269 questions with goals in areas of asset management, control management, configuration and change management, vulnerability management, incident management, business continuity management and risk

management (Bagheri, 2020). In Ireland, The SPEAR project tool was important as it had the ability to detect different kinds of attacks concerning confidentiality, integrity and availability, as well as timely detection of these attacks were key to their business model in the manufacturing sector (Rokkas & Neokosmidis, 2020). This included aspects such as speed and accuracy of detection which is the ability to detect and respond early to cyberattacks and accuracy of detection (Rokkas & Neokosmidis, 2020).

NIST (2021) developed a systematic cybersecurity framework as well as identified a few cybersecurity objectives for manufacturing. The five functions of the framework included threat and vulnerability identification, protection, detection, response, and recovery. Eilts (2021) explained that the cybersecurity Framework can be used to measure cybersecurity readiness and adoption. The framework consisted of five functions, namely identification, protection, detection, response, and recovery. Identification was an organizational activity to understand cybersecurity risks by conducting vulnerability assessments and controlling computer ports for the identification of cyber-attacks (Eilts, 2021). Protection of cyber infrastructure and services involved encrypting data and installing anti-virus software, and using strong passwords to protect IT infrastructure from cyber-attacks. Detection was the process of identifying cyber-attacks and could be carried out by organizations by conducting an operational and strategic analysis of incidents and monitoring security alerts regularly. To respond to cyber-attacks, organizations needed to have clear recovery plan procedures and backup databases.

However, attaining cybersecurity is complicated due to the fact that information systems exist in various physical, information, cognitive, and social layers of an organization (Wang et al., 2022; Mishra et al., 2022). Integrating the varying opinions of different management groups and other employees adds another layer of complexity to attaining organizational cybersecurity. Cybersecurity evaluation is also complex since security hazards can be located in several parts of an information system, such as computer networks, hardware, software, third-party providers, electronic devices, and human actions (Dimase et al., 2015). Since cybersecurity challenges are unpredictable, there might be no comprehensive solution to safeguard businesses from cyber hazards (Balakrishnan et al., 2018; Chen et al., 2019).

The various studies reviewed (Roege et al., 2017; Bodeau et al., 2018; Rokkas & Neokosmidis, 2020; Eilts, 2021; NIST, 2021) informed the adoption of cybersecurity measures namely threat and vulnerability assessment, protection, detection and recovery since these measures are critical in ensuring safety of an organization’s data and critical infrastructure.

1.1.3 Manufacturing Industry in Kenya

Manufacturing is the corner stone of Kenya's industrial sector (Chege, 2018). Kenya's Vision 2030 aims at the country's manufacturing industry becoming one of the key productive sectors identified to drive economic development and achieve the 10 percent annual growth target (KAM, 2021). The sector is expected to play a significant role in propelling the country to a path of sustainable growth in order to achieve Vision 2030. Manufacturing has enormous potential for wealth creation and capital accumulation, knowledge transfer, poverty reduction, and job creation (Government of Kenya, 2007). Manufacturing employment increased by 1.8 percent in 2016, accounting for 11.8 percent (300,800 jobs) (Kenya National Bureau of Statistics, 2017). However, the contribution of the manufacturing sector to GDP for the last 5 years has continued to decrease from the high of 9.4 percent in 2015 to the lowest of 7.5 percent in 2019 (KAM, 2021). The continuing decline in the contribution of manufacturing sector to GDP is a threat to the achievement of the policy target of 15 percent by 2022 as set in the Big Four Agenda (KAM, 2021).

Manufacturing firms in Kenya produce a wide range of goods and services and the Kenya Association of Manufacturers (KAM, 2021) directory identifies 14 key industrial subsectors. They include; Agriculture Sector, Automotive, Building, Mining and Construction, Chemical & Allied Energy, Electrical and Electronics, Food and Beverages, Leather and Footwear, Metal and Allied Paper, Pharmaceutical and Medical Equipment, Plastics and Rubber, Textile and Apparels Sector, Timber, Services and Consultants spread across major towns. Kenya's economy is still dominated by the service sector, which accounts for 53.56 percent of GDP. Kenya's manufacturing GDP contribution has steadily declined from 12.05 percent in 2011 to 7.6 percent in 2020 (World Bank, 2020). According to Were (2016), three elements related to technology in the manufacturing sector need to be analyzed. The first is the use of technology, the second is related to the manufacturing of technology products in Kenya and the third is the extent to which the large technology community in Kenya intersects with the manufacturing sector.

Manufacturing has become an increasing critical industry sector for reported cyber incidents (Dalal et al., 2022). According to Ransomware, cyberattacks amounted to losses in Africa in excess of 500 million dollars in 2021, while in that year ransom demands had escalated by 40% and malicious internet infiltration by more than 600% since 2020. Cyberattacks can lead to loss of product and process, production losses due to destroying, modifying, reprogramming parts and processes, damage to reputation, and even injury and loss of life (Sallos et al., 2019). Legacy hardware and software systems are commonly used in manufacturing processes and some of these systems were not designed with cybersecurity in mind (Manns, 2021). Annually,

Gartner releases their IT Key Metrics Data that tracks numerous various data points relating to technology trends and investment (Mangano, 2018). Manufacturing was at the bottom with only 4.3 percent of IT spend dedicated to cybersecurity, with all industries averaging out at 6.2 percent (Mangano, 2018). According to a global study, manufacturing was the second most targeted industry in 2019 right after healthcare (Weber & Kleine, 2020). According to the U.S. National Center for Manufacturing Science, variants of Trojans and droppers accounted for 86 percent of the malware in the manufacturing sector (Linkov & Palma-Oliveira, 2017).

Given the increase in the number of threats afflicting businesses both globally and locally, it is critical for the manufacturing industry to adopt cybersecurity to ensure survival. Again, due to the significance of asset security, manufacturing companies need to protect information and technology assets from cyber-attacks.

1.2 Statement of the Problem

The manufacturing industry has entered a digital renaissance where factories are requiring reinvention to address changes in customer demand, increased global competition, and organizational constraints (Oltramari et al., 2015). Manufacturing companies are now being forced to invest in information technology and cybersecurity efforts in a manner that is new and unfamiliar to the industry to address the digital divide as it expands in an industry that is slow to change and adapt (Johnston, 2022). Digital transformation of manufacturing processes leaves it vulnerable to cyberattack (Eian et al., 2020).

Cybercrime has led to the loss of billions of dollars, the malfunctioning of computer systems, the destruction of critical information, the compromising of network integrity, availability and confidentiality (Mphatheni & Maluleke, 2022). According to Morgan (2021), global financial losses due to cybercrime are expected to rise by 15 percent per year over the next five years. Serianu (2021) indicated a loss of about 3.5 billion US dollars globally and 649 million dollars in Africa. Six years ago, the total cost of cybercrime in Africa was estimated to be 3.5 billion dollars (Serianu, 2021). For instance, the government of Mauritius experienced a severe cyberattack in 2019 that harmed a number of government websites and systems (Serianu, 2021). During a cyberattack in 2020, the Ethiopian government's internet services were down for several days (Serianu, 2021). According to Serianu (2021), Nigeria, Kenya and Ghana were the top three African nations with the highest cyber threats. South Africa experienced 230 million cyberattacks between January 2020 and February 2021, while Kenya and Morocco experienced 72 million and 71 million cyberattacks respectively (Serianu, 2021). Despite the rising concerns about cybersecurity in Africa, many nations still require more infrastructure and resources to effectively combat cyber threats (Serianu, 2021).

Organizations need to consider appropriate factors in their decision-making process to handle cybersecurity problems. Studies conducted on adoption of cyber security have mainly focused on the challenges faced during cybersecurity implementation and success factors (Kent, 2016; Guidone, 2020; AL-Nuaimi, 2022; Choejey et al., 2016; Kovacevic et al., 2020). The studies concluded that the challenges faced become an obstacle by limiting the extent to which the strategic objectives are realized or they altogether hinder realization of any of the objectives of implementation resulting in a failure situation. This approach has been recently criticized as it does not provide a satisfactory explanation of which factors determine the adoption of cybersecurity measures. These researches were also conducted in different geographical areas and sectors and hence the findings may not be generalized to the Kenyan context. Studies in the area that do exist either have a high specific focus on other industries or focus on developed countries.

Wilem et al. (2021) found that factors such as information system compatibility, perceived usefulness, and perceived ease of use, influence the adoption of cybersecurity standards in Malaysia. However, other reasearchers argued that cybersecurity adoption goes beyond the detection of technological impacts and involves all the dimensions of an organization. The new approach now involves the management of organizational factors (Tejay and Klein, 2021). Many best practice standards and principles exist to reduce threats and improve cybersecurity, including the ISO/IEC 2000 series and National Institute of Standards and Technology (NIST 2022; Garba et al., 2020). However, cybersecurity guidelines are insufficient to resolve these problems (Rowe and Gallaher, 2016; Fischer-Hübner et al., 2021; Hejase et al., 2021).

Dhillon et. al (2021) conducted a literature review of the last 30 years of research about cybersecurity within the field resulting in a conceptual model that summarizes the research agenda of the phenomenon. This resulted in four categories that research usually falls within studies of structures, people, technology, and tasks. Further, these four categories can be divided into two groups that either study the structures and people or the technical systems (Dhillon et. al. 2021). These findings were consistent with the findings of Kabanda et al. (2018) study on South African SMEs cybersecurity implementation in developing countries, which identified organizational readiness as a critical aspect of cyber security adoption.

The study by Asiltürk (2022) found that senior management should have a greater ability to harden the organization cyber security defenses while also making the business more resilient. Nifakos et al. (2021) examined the critical success factors of cybersecurity in the health care sector in developed countries. The author noted that resources and management support were important drivers for the adoption of cybersecurity. The study by Mupila (2023) examined the factors that affect cybersecurity readiness as well

as technology readiness. These factors included management factors, organizational factors and environmental factors. While the necessity of having sufficient technology facilities should not be overlooked, similar emphasis should be paid to the non-technological factors influencing adoption of cybersecurity (Caras et al. 2019; Gyunka & Christiana 2017).

Manufacturing industry is one of the most vulnerable to remote cyber-attacks in Kenya (KAM, 2021). Due to the possibility of sizable reward or access to priceless data, large manufacturing firms are frequently the most alluring targets for cyber attackers (Eian et al., 2020). These organizations might also have IT infrastructures that are legacy systems and more complex which makes them more susceptible to cyber-attacks (Garba et al. 2022). Despite these studies being carried out on factors affecting adoption of cybersecurity, there are limited studies specifically focusing on manufacturing companies within the Kenyan context. Again, majority of the studies seem to have focused on the developed context other than a developing country like Kenya. This research gap highlights the need for a focused investigation into the adoption of cybersecurity factors within the large manufacturing companies in Kenya. By addressing this gap, the study aims to provide valuable insights and contribute to the knowledge base surrounding adoption of cybersecurity in the developing context.

To establish the factors that influence the adoption of cybersecurity, this study assessed three factors, namely technological factors, organizational resource factors, and management factors. The adoption of cybersecurity measures for this study were threat and vulnerability assessment, protection, detection and recovery which included activities both before, during and after a cyber-attack. The study seeks to pin-point the specific factors that need to be improved in order to increase cybersecurity adoption in the manufacturing industry in Nairobi.

1.3 Research Objectives

1.3.1 General Objective

The general objective of the study was to analyze the factors that influence the adoption of cybersecurity of large manufacturing companies in Nairobi County.

1.3.2 Specific Objectives

The specific objectives were:

i. To establish the effect of organizational resource factors on adoption of cybersecurity in large manufacturing companies in Nairobi County

ii. To establish the effect of management factors on adoption of cybersecurity in large manufacturing companies in Nairobi County

iii. To establish the effect of technological factors on adoption of cybersecurity in large manufacturing companies in Nairobi County

1.4 Research Questions

i. What is the effect of organizational resource factors on adoption of cybersecurity in large manufacturing companies in Nairobi County?

ii. What is the effect of management factors on adoption of cybersecurity in large manufacturing companies in Nairobi County?

iii. What is the effect of technological factors on adoption of cybersecurity in large manufacturing companies in Nairobi County?

1.5 Scope of Study

The study focused on the effect of management factors, organizational resource factors and technological factors on the adoption of cybersecurity on large manufacturing companies in Nairobi County. The study focused on 114 large manufacturing firms who were members of Kenya Association of Manufacturers (KAM, 2021). This was because there was an increase in cyber-attacks targeting large firms compared to other firms. KAM is the business member representing organizations for manufacturing value-added sector in Kenya. The study was specifically limited to those large manufacturing firms located within Nairobi and its environs. The study respondents were Chief Technology Officers, Chief Information Security Officers/IT Managers and ICT Officers/System Analysts/System Administrators. The theoretical scope was based on Human, Organization and Technology theory and General Deterrence theory.

1.6 Significance of the Study

The study is expected to be useful to various individuals, institutions and stakeholders. The study will provide security professionals with information that can be used to determine how to develop sustainable and flexible cybersecurity frameworks. The findings will also provide insight that can be useful to large manufacturing firm managers in charge of protecting critical assets as they provide guidance on the necessary investments that will increase their organization cybersecurity.

The study may also be of value to policy makers (such as the government) and regulatory bodies such as Communications Authority of Kenya, Office of the Data Protection Commissioner of Kenya and

membership bodies such as KAM and IRM which may trigger policy formulation aimed at improving the adoption of cybersecurity in large manufacturing firms.

The survey may also benefit scholars and researchers by expanding knowledge in the field of adoption of cybersecurity in large manufacturing companies which has limited literature and empirical evidence. The study will also serve as a reference for future scholars and researchers, as well as a foundation for future research.

1.7 Chapter Summary

The study focused on examining the factors influencing adoption of cybersecurity in the large manufacturing sector in Nairobi County. Despite a number of studies having been conducted on the key variables of the research, none of the examined empirical studies have combined the determinants selected in this study and examined factors influencing the adoption of cybersecurity of large manufacturing companies in Nairobi County.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter presented the literature review that covers previous literature relevant to the study. In this section, the study discussed other authors work and findings as guided by the research objectives. It also identified knowledge gaps that have yet to be filled. Based on the Human, Organization and Technology theory and General Deterrence theory, this section investigated the effect of organizational resource factors, management factors and technological factors on adoption of cybersecurity. Finally, the chapter presented the conceptual framework, which captured the hypothesized interaction between the variables in the study.

2.2 Theoretical Foundation

This study was anchored on The Human, Organization and Technology theory which informed the independent variables while the General Deterrence theory informed the dependent variable.

2.2.1 Human, Organization and Technology Theory (HOT)

The study derived the factors influencing the adoption of cybersecurity in organizations from Human, Organization Technology (HOT) theory. The HOT framework was initially developed for Health Information Systems (Yusof et al., 2008). The HOT framework is built on previous models of evaluation, including the IT-Organization Fit Model and the Information System Success Model (Miron & Muita, 2014). The framework propagates that the more technology, human and organization fit with each other, the higher the potential of Human Information System. The technology factors in HOT framework includes factors like system quality, information quality and service quality whereas the human factors in the HOT framework include factors like system use and user satisfaction (Model et al., 2023). Similarly, the organizational factors in the HOT framework include structure and environment (Badi, 2023).

The HOT theory is based on the premise that apart from technical issues, human and organizational aspects are also crucial in identifying the important factors for enhancing cyber-security in organizations ((Al-Hawamleh, 2023). Human factors that can influence cybersecurity includes the role of senior management and personality traits of the IT security manager (Rufai et al., 2020). Organizational factors of HOT theory include strategies adopted by the management of the organization (Rufai et al., 2020). Technological factors of HOT theory include technical measures adopted for enhancing cybersecurity (Rufai et al., 2020). The theory was relevant in the current study because it is a multilevel model that incorporates the technological

factors, organizational resource factors and management factors influencing the adoption of cybersecurity measures.

2.2.2 General Deterrence Theory

The emergence of deterrence in military theory dates back to the 1920s and 1930s when the first flight bombers were considered unstoppable by defensive measures (Bendiek & Metzger, 2015). Deterrence theory gained prominence and developed to its present state during the Cold War nuclear stand-off between the USA and the Soviet Union (Dunn et al., 2023). Deterrence is concerned with discouraging others from acting in ways that advantage them but harm you (Farheen Ansari, 2022). The General Deterrence Theory advocates the use of strong deterrents and penalties to dissuade people from doing malpractices and perpetrating cyber-attacks. The four main elements of the General Deterrence Theory are threat identification, protection, detection, response and recovery (Senarak, 2021b).

The strong defense network of public and private Computer Emergency Response Teams (CERT) is one component thereof (Plessis, 2021). However, distinguishing between offence and defense is not always easy since evaluating one's own defenses requires penetration-testing and thus the ability to intrude into systems (Mwangi et al., 2022). Other researchers (Andronache, 2021; Lavicza et al., 2021; Schatz et al., 2017) strongly disagree with the emphasis on defense, arguing that in an offense-dominant environment, a fortress mentality will not work. In cyberspace, lack of clarity and credibility of punishment encourages cyberattacks to test defenses and push their limits, defying deterrence-by denial (Andronache, 2021).

Counter measures that include training and education, backups and disaster recovery measures can be adopted to eliminate the threats and mitigate against such risks (Van et al., 2014). Deterrence activities promote activities that counteract criminal abuse of cyberspace through awareness initiatives for cyberspace users (Alanezi, et al., 2014). Hence, stiff punishment and awareness programs deter many potential perpetrators. Authors in Cheng et al. (2014) found that employees focus on the perceived benefits of personal internet use while, at the same time finding justification for their behavior and keep less attention to the expected punishment. They are less worried about severity of punishment, and more worried about the likelihood of being caught (Schuessler, 2009). This theory propositions that individuals can be discouraged from committing irregular selfish acts through the use of counter measures which include strong deterrents and sanctions comparative to the act (Schuessler, 2009). Counter measures such as education and training, back-ups, insurance and disaster recovery measures could be put in place to eliminate some threats or at least mitigate such risks (Schuessler, 2009).

According to the General Deterrence Theory (Williams & Hawkins, 1986), the severity of legal sanctions could deter individuals from indulging in criminal activities. Roumani et al. (2015) and Chen et al. (2011) also found that attackers regularly probed organizational networks to recognize software vulnerabilities that are not patched by users, and eventually exploit them. This theory applies to the adoption of cybersecurity measures through having a strong cyber defense relative to the information security strategic assets involved thus making an attack exceedingly difficult relative to returns (Doche et al., 2019). General deterrence theory provides means or strategies for managers to analyze the continuous defense measures to be employed and direct investments to the most impactful defense measures. The theory was also useful in explaining how organizations change and adapt policies and processes in response to the cybersecurity environment to adopt cybersecurity measures

The theory also relates to this study as it informs systems administrators and managers that a system defense should be relative to associated assets such that the cost of the attack is also high thus a deterrent to cyber-attacks (Njenga & Jordaan, 2016).

2.3 Empirical Review

This section presented a review of previous studies conducted at global, regional and local level on the factors influencing the adoption of cybersecurity. The section was divided based on the study objectives that was organizational resource factors and adoption of cybersecurity, management factors and adoption of cybersecurity, and technological factors and adoption of cybersecurity.

2.3.1 Organizational Resource Factors and Adoption of Cybersecurity

Organizational resource factors refer to characteristics of an organization, including organizational structure, policies, decision-making processes, employee knowledge and cultural issues (Bagheri, 2020). It also refers to the resources that an organization provides in the adoption of cybersecurity (Davies, 2017). Building awareness is only one aspect of organizational support. It also includes motivating employees and developing effective, understandable, and simple-to-implement policies (Pitichat, 2015). Organizational resource factors may influence the adoption of cybersecurity culture and frameworks (Hameed et al., 2017; Narain et al., 2014; Zammani et l. 2016). Several studies that have been conducted consistently state that there are two types of company resources, namely tangible and intangible. In previous studies, it is generally explained that tangible resources are divided into two types, namely financial and physical, while intangible resources such as knowledge, ability to innovate, trademarks, marketing capabilities, and intellectual capital of employees skilled (Noparumpa et al., 2021).

One of the challenges in cybersecurity management is the optimal allocation of limited resources among competing assets and vulnerabilities threats (Banga & Willem, 2018). A cost benefit model is adopted to determine resource allocation to various assets and vulnerabilities threats. Organizational resources include labor, Internet of Things assets, and financial resources, and these are translated into monetary terms (Banga & Willem, 2018). It was noted that there have not been any resource allocation methods used for cybersecurity investment decisions (Banga & Willem, 2018). Previous studies confirm that the availability of resources and capacity and resource platforms leads organizations to adopt cybersecurity measures.

Jalali et al. (2019) explored the organizational perspective of cybersecurity in the healthcare sector. The study followed a systematic literature review and focused on the most important aspects required to successfully adopt cybersecurity in healthcare. The study highlighted and focused on organizational factors that also touch on healthcare institutes' technical readiness. Software development security, disaster recovery planning and business continuity were the factors identified in this study. The research focused on organizational and technological factors of the healthcare industry. This study looks at how management factors influence adoption of cybersecurity in the large manufacturing industry.

In another research, Khansa et al. (2017) conducted two rounds of a qualitative survey to investigate the impact of organizational control in the cyber environment in Finland. The study focused on the relationship between employee cyber loafing and formal organizational control. Employees who surf the internet for personal reasons during work hours are said to be cyberloafing. Such behavior reduced productivity and may lead to unwanted and serious security issues. According to the study, attitudes, subjective norms perceived, behavioral controls, and a lack of punishment all play an important role in designing organization controls that must be considered for any given cybersecurity standard. The methodology used by Khansa et al. (2017) differs significantly from the techniques used in the current study.

In another research in Amsterdam, Peursum (2015) studied the building blocks necessary for a security strategy from an organization perspective. The researcher adopted an expert interviews methodology to confirm data collected from the literature. The key factors highlighted were, systems, skills, staff, strategy, style shared value and structures. Kreicberga (2013) conducted a study on internal security threats to information safety countermeasures on human factors in small businesses in Sweden. According to the findings, formal policies lack appropriate safeguarding and awareness means and thus do not affect employee behavior, whereas casual norms within organizations have the most control over information security behavior.

Trim & Lee (2022) investigated how organizational structures and systems are interconnected and used to improve an organization's cybersecurity knowledge development. The researchers employed a qualitative research strategy that includes group interviews with cybersecurity and intelligence experts. The mind map approach is employed to recognize senior managers' thought processes in terms of ensuring the effectiveness of the cybersecurity management process. According to the study, senior managers can use the global cybersecurity model to establish a framework for dealing with a variety of cybersecurity attacks, as well as to improve individuals' cybersecurity skill and knowledge base. The methodology utilized by the researcher differs significantly from the techniques employed in the current study. In Greece, Security Awareness and Training Program Specific knowledge, skills, and abilities' identification needed to support defense of the organization, development and execution of an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs (Georgiadou et al., 2022).

Financial investment is a key factor for any organizational capability. IT and cybersecurity are no different, especially with technology evolving as frequently as every 12-18 months. In a 2016 study conducted jointly between Deloitte and the manufacturers alliance for productivity and innovation, 225 executives were interviewed regarding cyber-risk in advanced manufacturing. From the responses, it was determined that only 52 percent were confident that the proper protections had been put in place against external threats. Appropriate funding and talent readiness were cited as the key reasons for the lack of confidence. Furthermore, 48 percent of the respondents noted that funding was not adequate for the necessary cyber initiatives and 27 percent detailed that there was a lack of senior level support (Akpan et al., 2022).

Kannus et al. (2018) focused on the cybersecurity in the organization with a focus on the sectors of power distributions, railway and health care. The study employed a case study approach to investigate the factors that influence the cybersecurity posture in the aforementioned domains, either directly or indirectly. Competence, compliance, awareness, leadership engagement, and system technology management were the key factors outlined in this study. This is a cross-industry investigation, whereas the current study establishes the factors influencing cybersecurity adoption, specifically in large manufacturing companies.

The findings presented above were consistent with those of Kabanda et al. (2018), who investigated how SMEs perceive cybersecurity in South Africa and the factors that influence the techniques that they employ. The purpose of this study was to investigate SME cybersecurity practices and the challenges they face in developing countries. The study employed a qualitative inquiry approach to gather information from three South African SMEs that have implemented cybersecurity practices. The findings showed that SME's

perception of cybersecurity is hampered by internal budget constraints. This study did not examine how management factors and technological factors influence adoption cybersecurity.

Nifakos et al. (2021) reviewed current literature on the role of humans in strengthening cybersecurity defenses within health care organizations. A total of 70 articles was selected to be included in the review from a total of 695. To collectively strengthen healthcare organizations against ever-increasing cyber threats, the study concluded that a collaborative and standardized approach for the development of training programs, awareness campaigns, and information sharing on the nature and type of cybersecurity attacks is required. The previous study examined the literature whereas the current study will collect primary data.

Kent et al. (2016) examined the cybersecurity phenomenon from the perspective of South African SMEs. The purpose was to investigate the factors that influence SMEs cybersecurity implementations. Using a qualitative approach and interviews to collect data, the findings showed that the type of cybersecurity measures implemented within a SME is determined by organizational readiness. SMEs were more vulnerable to cybersecurity threats because they only adhere to the most basic cybersecurity standards and regulations. All other possible cybersecurity strategies were frequently ignored and underutilized. SMEs admit to lacking the necessary skills and financial resources to address cybersecurity concerns. The study failed to examine how technological factors impact the adoption of cybersecurity. This study will establish how these factors interact and their impact on the adoption of cybersecurity.

In Cameroon, Nikel et al. (2022) study examined the adoption of non-technical countermeasures to manage cybersecurity in organizations. The data was collected from 214 participants. A descriptive statistic percentage result showed that less than half of respondents have completed or are enrolled in a regular training program. According to the study, more than 61 percent of participants were unaware of their organization's cybersecurity policies. Among other findings, the fact that more than 60 percent of employees' errors or violations of security policy were not disciplined or penalized demonstrates the legal status of cyber-attacks. According to the study, organizations in Cameroon should invest in cybersecurity education for their employees, with a focus on communication, engagement, collaboration, and social engineering. The study also recommended prioritizing the development and implementation of a cybersecurity strategy to serve as the foundation for policies and other security efforts.

Locally, Wechuli (2014), Makumbi et al. (2012) and Nyamongo (2012) analyzed the restraining factors affecting these frameworks, assessment of IT technology security related practices within small enterprises

in the financial Sector in Kenya and information systems security management on private chartered universities in Kenya respectively. Their objectives were to establish factors affecting cybersecurity within government ministries, the level of dependence on Kenyan SMEs are on ICT and to find out how Kenyan small enterprises and medium enterprises are safeguarding their systems and networks from data theft respectively. The three studies agreed that security information awareness and training in organizations and institutions should be prioritized and that a robust strategic security measure should be implemented in managing cybersecurity.

According to the studies, organizations need to implement numerous security strategies such as functional separation, security access controls, and investments in IT assets, as well as user awareness campaigns to educate them on ICT security. Njiru (2013) added to what other scholars have done by conducting research on a framework guide to information security creativity for accessing banking information systems, a situation in the Kenyan banking sector. The study's main aim was to identify common vulnerabilities affecting banking information systems and frameworks used to evaluate security programs in banking systems (Njiru, 2013). According to the findings, people were the greatest threat to information security and a lack of proper training and awareness among staff and customers are the major impediments to security effectiveness. This research focuses on the financial industry. The current study will concentrate on the large manufacturing companies.

2.3.2 Management Factors and Adoption of Cybersecurity

Management factors refer to high level executives' direct involvement and push toward strategic goal realization (Zwikael & Meredith, 2019). It entails taking part in the transformation of policies and objectives into goals and projects (Ahmed & Philbin, 2022). Managers' influence, according to Nyesemane (2021), is an important aspect of strategic goal execution because these individuals are usually in charge of making decisions that affect everyone in the organization. According to Mandal (2020), in order to implement changes within an organization, managers need to psychologically prepare employees and explain the significance of the change and how it will impact their jobs. Management is critical in implementing changes, and in manufacturing companies, management support is critical in approving funds and other resources for cybersecurity adoption (Bagheri, 2020). Managers can also help with cybersecurity by providing employee training programs, motivating employees to adopt change practices, and reducing employee resistance to change (Turk et al., 2022).

Richardson et al. (2020) investigated how the human factor is the main reason for many successful attacks on school computers and systems in the United Stated since the uneducated computer user is the weakest link targeted by cyber criminals using social engineering. Employees were identified as the first line of defense for the school cybersecurity system in the study (Zammani & Razali, 2016). The researchers noted that if the leadership of a school demonstrates and instills the importance of cybersecurity and good cyber behavior, the mindset may rub off on employees and improve the culture.

Asiltürk (2022) determined the significant interaction between senior management and the IT team in the successful continuation of the strategic cyber intelligence process in United Stated enterprises. Most large businesses were beginning to view cybersecurity initiatives from a more corporate perspective, involving teams led by the CEO, CISO, CIO, and CRO. Many senior executives view cybersecurity as a technical issue and delegate it to the IT department as a result. However, beyond a technical issue, the IT department may be unable to properly fulfill its cybersecurity responsibility because it involves various elements of an enterprise as a whole, such as risk culture, value chain, business model, and company management (Poppensieker and Riemenschnitte, 2019). According to the researcher, such divisions were obsolete in the digital age and the scattered responsibility of divisions can put the entire organization at risk.

In Japan, Aoyama et al. (2015) study evaluated the human contribution to cybersecurity in the field of critical infrastructure security in the manufacturing industry. The researchers used an observation method in which participants were split into offensive and defensive teams. The latter functions as a single organization, with members assigned to roles such as manager, factory operator, and IT administrator. When a management system failed to handle a situation, the researchers observed an increase in decision-making privilege, as well as a shift in control mode, and the core decision maker shifted from top management to each division, then to individuals.

Whitehead (2020) analyzed the perceptions of senior managers and owners of SMEs to understand the factors that influence decision making related to additional cybersecurity investment. According to the researcher, cybercrime was especially important for SMEs with limited budgets to protect themselves. To best answer the research question and achieve all research objectives, a qualitative approach using semi-structured interviews is chosen. Purposive sampling was used to select five participants who met the outlined criteria. Thematic analysis is used to analyze interviews, and findings are critically evaluated in the context of existing literature. The six factors influencing cybersecurity investment decisions SMEs were identified as cost, company reputation, monetary loss, awareness, regulation and expertise. Critically, this research showed that

SMEs acknowledge the need to invest and are willing, but more guidance is required to ensure investment targets the areas most impactful for the business

Shreeve et al. (2022) analyzed how managers make cybersecurity decisions. The researchers examined the decision-making conversations of seven teams of senior managers from the same organization as they complete the Decisions & Disruptions cybersecurity exercise. The study employed grounded theory to contextualize their decision-making analysis and to investigate how these complex socio-cognitive interactions occur (Shreeve et al., 2022). The study demonstrated how managers with little cybersecurity expertise can make cybersecurity decisions using logic and traditional risk management thinking (Shreeve et al., 2022). Despite their lack of cybersecurity training, they exhibited reasoning that closely resembles the decision-making approaches advocated in cybersecurity standards. Finally, non-cybersecurity experts can create a cybersecurity model based on their current situation and update it as new requirements emerge or new incidents occur), while capturing their reasoning at each stage.

2.3.3 Technological Factors and Adoption of Cybersecurity

Technological factors are the features that affects adoption of cybersecurity (Davies, 2017). Research on the technological factors is mainly focused on either the technology or the design of the systems (Dhillon et. al., 2021). Awan et al. (2017) investigated cybersecurity strategies for overcoming security measures in Pakistan. The researchers identified the effective factors that influence the success of implementing such cybersecurity strategies to circumvent such safeguards. The factors emphasized in a systematic literature review were the level of governance in critical information infrastructure, the level of protection, the sharing of cybersecurity information, and insufficient market preparation. The implementation of the new cyber infrastructure included IoT cyber technology development, testing, deployment, new policy development, training, and user acceptance (Banga & Willem, 2018).

According to the Technology, Organization and Environment framework, technology represents an organization's technological readiness that includes its IT infrastructure and IT personnel that impact adoption decisions (Depietro et al., 2017; Zhu & Kraemer, 2018). In addition, technology can include how well an organization has integrated technology (Wang et al., 2010). Finally, the technology dimension includes an organization's readiness to embrace technology and which technology is available and relevant to its needs. Naik (2022) study mainly focused on challenges faced by cybersecurity on the latest technologies in India. The study discovered that the most recent and disruptive technologies, as well as new cyber tools

and threats that emerge on a daily basis, are challenging organizations not only with how they secure their infrastructure, but also with how they require new platforms and intelligence to do so.

Abdalla et al. (2021) investigated the factors influencing the adoption of cybersecurity standards among Malaysia's publicly listed companies. An online survey was distributed to 275 publicly traded companies. According to the findings, the use of expected related benefits had a significant impact on the adoption of cybersecurity standards. On the other hand, perceived security had a significant moderating influence on the relationship between organizational factors and cybersecurity standard adoption. In the United Stated, Manns (2021) investigated the relationship between perceived vulnerability, perceived severity, and perceived benefit on cybersecurity adoption in SMEs. The theoretical foundation for the research in this study was the protection motivation theory. 90 percent of registered businesses in the United Stated are small to medium-sized businesses. According to the findings of this study, SMEs understood what factors influence cybersecurity acceptance and how employees perceive the risks associated with technology use. This study revealed a significant relationship between prior cybersecurity acceptance and perceived vulnerability.

In Korea, Ghelani (2022) investigated how businesses use security techniques to protect their information systems. The study revealed a deeply ingrained preventative mindset motivated by a desire to ensure the availability of technology and services as well as a general lack of awareness of enterprise security concerns. The research looked at how to combine, balance, and optimize systems across an enterprise. Security strategies have been identified, including prevention, deterrence, surveillance, and detection. To determine how these security strategies are used in organizations, a qualitative focus group approach was used. Security managers from eight organizations were asked to participate in focus groups to discuss their organizations' security strategies. According to the findings, many organizations use a preventive approach to ensure the availability of technology services (Ghelani, 2022). On an operational level, some of the other identified methods were used to support the prevention strategy.

Kannus et al. (2018) investigated the cybersecurity landscape in Finnish manufacturing companies. According to the Delphi study, the most important drivers for the cybersecurity of the manufacturing industry in 2021 were identity and access management, ensuring availability, internet of things, digitalization, industry 4.0, and industrial automation security. Deshpande et al. (2014) conducted studies in India on cybersecurity, focusing on the strategy to security challenges and cybersecurity automation for regulating data distribution, respectively. Their findings were similar whereby, users needed to protect personal computers as well as other electronic devices. Firewalls can be used to secure all personal devices. According

to the studies, cybersecurity plays an important role in information systems and data distribution, and specific developed software must be developed using various mechanisms developed and used by scientists to protect information from attackers.

Glory et al. (2017) investigated the empirical literature on the adoption of cybersecurity and existing research gaps. The purpose of this study was to empirically investigate cyber technology adoption in order to understand how to influence operational adoption across the government sector and what can be done to develop a model that enables cyber technology adoption. The researcher found that getting organizations and individuals to commit to piloting a technology on a network remains difficult, especially when attempting to integrate technologies into existing government networks, processes, and business cycles. Potential users were worried about being the first to try a new capability, as well as failing. Catota et al. (2018) conducted research on the cybersecurity incident response capabilities in the Ecuadorian financial sector and found that one of the barriers that Ecuadorian financial institutions face that prevents them from properly responding to security is inadequate security controls and lack of technologies.

In Nigeria, Ibikunle et al. (2013) focused on the challenges and explanations for cyber safety issues in their study. The researchers discovered that there was a greater need for addressing ICT network vulnerabilities, implying the importance of cultivating a strong cybersecurity tradition and establishing cybersecurity partnerships between private and public organizations. Kayode et al. (2016) conducted research on cost benefit analysis of cybersecurity system investments in Nigeria. Costs and benefits were expressed in monetary terms and adjusted for the time value of money so that all benefits and costs are expressed on a consistent basis over time. Individuals from academia, financial institutions, and internet service providers are interviewed about the effectiveness, advantages, and disadvantages of the various security strategies they use. Mathematical models are developed and implemented, software was created to replicate the behavior of the models, allowing the costs and benefits of the cybersecurity strategies employed to be estimated by entering the monetary values associated with those security mechanisms. The model was also simulated using the Java programming language, primarily to assist users in performing a cost-benefit analysis of their specific choice of cybersecurity strategy.

Bernik et al. (2016) assessed the information security performance in organizations. The study found that technical and logical control were critical success factors in ensuring that an organization has the appropriate security posture and is prepared to prevent, detect, and respond to threats. The researchers recommended that cybersecurity evolves in a systematic manner, with the first steps including technical and logical security

controls to ensure that organizations can effectively respond to security incidents. Bonnevier et al. (2018) investigated the role of firewalls in network security and discovered that the majority of firewall configurations do not match the organization's security policies and that some organizations do not have any firewall configurations set. Most firewalls lack configurations due to a lack of understanding of the organization's policies or a lack of firewall policies. In general, if a firewall allows an unauthorized agent to access internal systems or information, it should be considered to pose a risk to information security because malicious networks are accessed by the user while the firewall remains unnoticed.

2.4 Research Gaps

These studies showed a significant influence of various factors on adoption of cybersecurity. However, these studies failed to investigate the specific context that the current research will examine, hence presenting a gap that this research will fill. Most of these studies were not carried out in Kenya. Such studies included Jalali et al., 2022; Fritzvold, 2017; Glory et al., 2017; Ghelani, 2022). While Whitehead (2020) reported the importance of management support in cybersecurity enhancement, the researcher failed to examine how organization resource factors and technological factors influence the adoption of cybersecurity. Other studies employed in industries that this study did not investigate, including Nifakos et al. (2021), who investigated health care cybersecurity, and Kent et al. (2016), whose focus was on SMEs. The study by Richardson et al. (2020) also investigated cybersecurity in schools. There appears to be a scarcity of studies that focus solely on the combined influence of technology factors, organizational resource factors, and management factors on cybersecurity adoption in the large manufacturing industry. This study fills the above gap. Table 2.1 below presents a summary of the gaps.

Table 2.1: Summary of Empirical Studies and Gaps

Author	Title of study	Findings	Research gap	Response to research gap
Jalali et al. (2019)	Health Care and Cybersecurity: Bibliometric Analysis of the Literature.	Found that organizational and technological factors influence adoption of cybersecurity in the healthcare sector.	The research was based on the health industry while the current study investigates the manufacturing industry. The study also fails to investigate how management factors affect the adoption of cybersecurity.	This study will expand the scope by assessing the impact of management factors influencing the adoption of cybersecurity within large manufacturing firms.
Kabanda et al. (2018)	Exploring SME cybersecurity practices in developing countries.	Found that SMEs adoption of cybersecurity is constrained by internal factors of budget.	This study failed to assess how management and technological factors affect the adoption of cybersecurity.	The current study will expand the scope by evaluating the impact of management and technological factors influencing the adoption of cybersecurity within large manufacturing firms.
Kent et al. (2016)	How South African SMEs address cybersecurity.	Found that organization readiness determines the type of cybersecurity measures	This study collected interview data and utilizes thematic analysis. The study focuses on South Africa, which is geographically and	The current study will utilize a descriptive method.

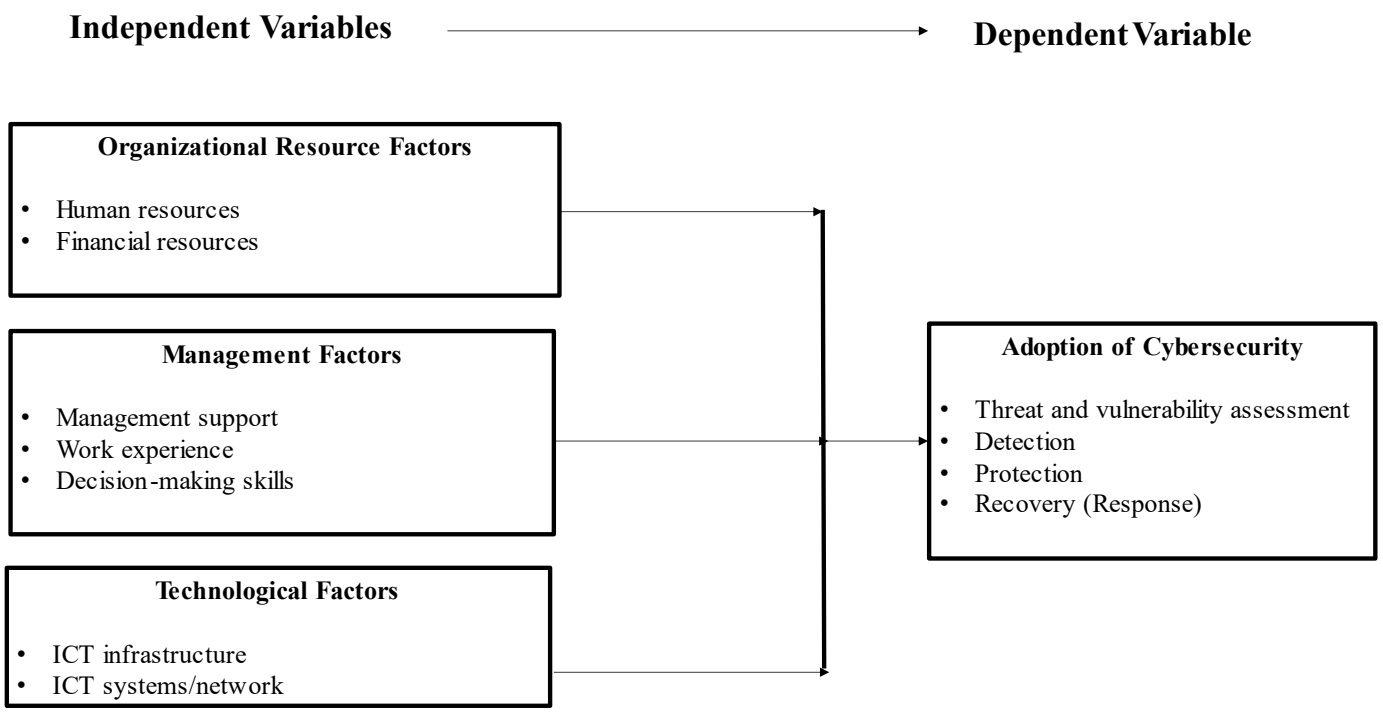
		implemented within an SME.	demographically different from Kenya.	
Richardson et al. (2020)	Planning for Cybersecurity in Schools: The Human Factor.	Found that employees are the first line of defense for the school cybersecurity system.	The research was based in the school industry while the current investigates the manufacturing industry.	This study will address some of these factors within large manufacturing companies.
Bagheri (2020)	Investigating Organizational Aspects of Cybersecurity in Large Organizations	Findings indicate that management and organizational factors play a key role in developing cybersecurity in universities.	The study collected interview data from two Australian universities.	This study will expand the scope by evaluating the technological factors influencing adoption of cybersecurity in large manufacturing firms in Nairobi County.
Justin et al. (2023)	Cybersecurity culture in an IT company: An empirical study	Findings indicate that policy factor, behavioral factor, consciousness factor, preventive factor, technology factor and effective measures is essential in creating a strong cybersecurity culture	The study was specific to start-up companies in India.	This study will address some of these factors in the manufacturing industry in Nairobi County

2.5 Conceptual Framework

A conceptual framework is a structure thought to be the best way to explain the natural progression of the phenomenon that the researcher wishes to study. It connects the general idea to the concepts, empirical

research and theories used to describe the study (Adom et al., 2018). In this study, the independent variables were organizational resource factors, management factors and technological factors while the dependent variable was the adoption of cybersecurity.

Figure 2.1: Conceptual Framework



Source: Researcher (2023)

The operationalization of the study variables is shown in the table 2.2 below:

Table 2.2: Operationalization of Variables

Variable	Type of Variable	Indicators	Scale	Source	Data Analysis
Organizational resource factors	Independent	• Human resources • Financial resources	Ordinal 5-point Likert scale	(Vries, 2017; Garba & Bade, 2021; Noparumpa et al., 2021; Opoku-ahene, 2022)	Descriptive and Inferential analysis
Management factors	Independent	• Management support • Work experience • Decision making skills	Ordinal 5-point Likert scale	(Andronache, 2021; Geil et al., 2018; Khansa et al., 2017; Kumar et al., 2021; Mwaniki et al., 2022)	Descriptive and Inferential analysis
Technological factors	Independent	• ICT infrastructure • ICT network/systems	Ordinal 5-point Likert scale	(Awan et al., 2017; Cheong et al., 2023; Kilani, 2020)	Descriptive and Inferential analysis
Adoption of cybersecurity	Dependent	• Threat and vulnerability assessment • Detection • Protection • Recovery (response)	Quantitative	(Tran et al., 2016; Roege et al., 2017; Bodeau et al., 2018; Eilts, 2021; NIST, 2021)	Descriptive analysis

Source: Researcher (2023)

2.6 Chapter Summary

This chapter has discussed the theoretical literature underpinning the factors influencing the adoption of cybersecurity in large manufacturing companies. Various theories of cybersecurity adoption were also reviewed. Lastly, the empirical framework of the current study has been discussed, research gaps identified and the variables of this study operationalized.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlined the research methodology that was employed to achieve the study objectives. The section outlined the research philosophy, research design, the target population of the study, sample size determination, sampling technique, data collection methods, data analysis techniques, research quality, and ethical considerations in the research.

3.2 Research Philosophy

Research philosophy is a set of assumptions and beliefs about the growth of knowledge in a specific field (Cook, 2017). There are four classic types of research philosophies, namely, pragmatism, positivism, realism and interpretivism (Oltramari et al. 2015). Pragmatism research philosophy accepts concepts to be relevant only if they support action through use of a combination of quantitative and qualitative data (Lobato, 2016). Positivism posits that only knowledge (facts) acquired through observation is trustworthy (Wu et al., 2018). Positivist philosophy restricts the researcher to data collection (using quantitative strategies) and deductive interpretation in an objective ontology (Cook, 2017). Interpretivism philosophy is the opposite reflection of positivism in that it adopts induction method and subjective ontology (Lykou et al., 2019). Finally, realism acknowledges that there is independence of reality from the human mind (Saunders et al., 2012).

As such, a positivist philosophy was adopted since the study sought to investigate relationships between components in the phenomena using a scientific approach (Kothari & Garg, 2014). When employing positivist research philosophy, one must choose between ontology and epistemology. In this case, epistemological positivism will be used, which is research thought that views observable evidence as the only form of scientific findings that can be defended. Additionally, the philosophy was adopted since the study aimed to investigate world phenomena without interfering with it.

3.3 Research Design

The research design provides a framework for organizing research work activities such as data generation and collection to answer research questions (Ehrari et al., 2020). A quantitative study collects numerical data to demonstrate the relationship between theory and observable social reality (Doche et al., 2019). The current study used a descriptive study design because it allows for quantitative approaches to be used in data analysis. Cross-sectional design was applied since data from respondents was collected across firms at a single point in time and within a short period. Furthermore, the study design allows for the examination of the study variables at a specific time with minimal intervention from the investigator, fostering neutrality in

understanding how the variables interact with one another (Bouwens & Stafford, 2019). The descriptive research design was used in this study to quantify any relationship that exists between the study's independent and dependent variables. This study's independent variables were organizational factors, management factors and technological factors. This study looked into how these variables affect the dependent variable, which was the adoption of cybersecurity in large manufacturing companies in Nairobi County.

3.4 Population of the study

According to Bryman (2016), a population is the universe of units from which a researcher wants to conduct an investigation. The target population of this study was primarily the large manufacturing companies in Nairobi County. According to the Kenya Association of Manufacturers (2021), 114 manufacturing companies are categorized as large companies. The population was chosen by the researcher to be the 114 large manufacturing companies.

3.5 Sampling Design

A sample, according to Kothari and Gaurav (2014), is a small proportion of an entire population, that is, a selection from the population. Purposive sampling, also known as judgmental sampling is a non-probability sampling technique in which the researcher actively chooses the sample based on certain criteria. Judgmental sampling was used to select 2 respondents who were from the sampled 114 large manufacturing firms. In this research, purposive sampling comprised respondents that had the capacity to offer reliable information based on their knowledge or experience in adoption of cybersecurity. The respondents comprised of Chief Technology Officers/Chief Information Security Officers/IT Managers and IT Officer/Systems Analysts. This accounted for 2 respondents per company in the 114 large manufacturing companies in Nairobi County bringing the sample size to 228 respondents. The sample frame for this study consisted of employees of large manufacturing companies operating within Nairobi County. The selection of Nairobi County was informed by over 80% of manufacturing companies based in Nairobi (KAM, 2021).

3.6 Data Collection Methods

The study dominantly relied on primary research data that was collected using a structured research questionnaire. The research questionnaire was divided into three sections and was designed in accordance with the study's literature and conceptualization of the study variables. The questionnaire was used in the survey because it was simple to collect information from a large population and used a systematic approach to data collection, making tabulation and interpretation of the results easier. The Likert scale allowed the study to evaluate the various dimensions and intensity of the respondents' attitudes toward the items as they

relate to adoption of cybersecurity in large manufacturing companies. This study employed a five-point Likert scale, with a score of 5 indicating strong agreement and a score of 1 indicating strong disagreement. The questionnaire was preferred because it is efficient, inexpensive, and simple to administer, it is relatively simple to analyze and it is simple and quick for respondents to complete and collect data in a standardized manner (Kothari, 2011).

The measurement instrument for this study was a self-administered questionnaire distributed through Google forms, though physical data collection might be possible. For reliability, online questionnaires were less expensive and more convenient to reach out to respondents with a link to the survey delivered through their official email addresses. An online survey allows respondents to complete it in their spare time, from anywhere, and at their own pace, which is likely to increase the response rate (Bryman, 2016). Where online contact is not possible, printed questionnaires were delivered and responses collected.

The researcher and research assistant called the respondents to introduce themselves and the study's objectives. Following that, respondents who agreed to participate in the study were sent the link to the online survey through the respondents' institution's official email address. To ensure reliability, the survey link was sent through the respondent's official email address. The researcher and research assistant contacted respondents who had not responded within a week of receiving the questionnaire. The printed questionnaires were used to collect responses from those who did not complete the online survey.

3.7 Research Quality

Testing and validity were used to ensure the research quality.

3.7.1 Validity Tests

The extent to which an instrument measures what it is supposed to measure and performs as it is designed to perform is referred to as its validity (Winterstein, 2008). The researcher determined the validity of the research instrument by soliciting the opinions of experts in the field of study, particularly the researcher's supervisors, quality experts and lecturers. These experts reviewed the instruments to determine whether they were adequate and valid enough to collect data/information to answer the study's objectives, ensuring the instrument's face and content validity. The experts' feedback assisted with the necessary revisions and modifications to the research instrument.

3.7.2 Reliability Tests

This is the degree to which a research instrument can consistently assess a characteristic of interest (Meeker & Escobar, 2014). A researcher seeks to ensure as little variation as possible in the results of the research instrument and study methodology when testing reliability (Kotter, 2012). Cronbach's alpha coefficients was computed to establish the survey's reliability for all items in the questionnaire, as well as the overall evaluation given (Kabanda et al., 2018). To assess internal consistency, the Cronbach (1951) Alpha test was run on IBM SPSS. Cronbach's Alpha coefficients typically range from 0 to 1, with a higher alpha coefficient value indicating greater reliability. The acceptable value of 0.7 was used as the reliability cut-off in this study. Results presented in table 3.1 indicate that all the variables attained the acceptable and recommended level of alpha 0.50.

Table 3.1: Test of Reliability of the Research Instrument

	Reliability Statistics	
Constructs	**Cronbach's Alpha**	**N of Items**
Adoption of Cybersecurity	0.7482	12
Organizational Resource Factors	0.7239	12
Management Factors	0.7710	7
Technological Factors	0.7088	3

Source: Researcher (2023)

Based on these scores, the findings showed the study variables were within the acceptable range of internal consistency hence no further amendments were required in the research questionnaire.

3.8 Data Analysis

According to Saunders et al. (2019), data analysis is the process of drawing conclusions about the relationships between the data variables that the research is designed to test in order to answer the research questions and objectives. Saunders et al. (2019) notes that some findings may be discovered that were not initially planned for and are thus important to report. The researcher reviewed completed questionnaires to ensure their accuracy and relevance. The responses were downloaded from Google forms, while the physical copies were converted to excel format and cleaned. The study's data analysis tools were IBM SPSS and Microsoft Excel. The analysis of data also employed both descriptive statistics and inferential statistics. Descriptive statistics included measures of central tendency (the mean) and measures of variability (standard deviation). In terms of inferential statistics, both correlation analysis and regression analysis were conducted

as part of the study. Correlation analysis assessed the suitability of the research variables for further investigation.

Spearman Correlation analysis was used to determine the relationship between the adoption of cybersecurity of large manufacturing companies and the factors influencing adoption of cybersecurity in manufacturing companies. The evaluation criteria were as follows: a correlation coefficient ranges between the values +1 and -1. A value of -1 implies that there is a perfect negative correlation, a value of 0 implies no correlation and a value of +1 signifies a perfect positive correlation. According to Schober et al. (2018), a correlation value of below 0.20 is interpreted as a very weak correlation, a range of 0.20 to 0.39 is weak, 0.40-0.59 is moderate, 0.60- 0.79 is a strong correlation and 0.80-1.00 is a very strong correlation. To determine the relationships between the variables in the study, a multiple regression analysis was carried out.

The multiple regression model adopted was:

$Y = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \varepsilon$ Equation 3.1

Where:

Y = adoption of cybersecurity

X_1 = organizational resource factors

X_2 = management factors

X_3 = technological factors

$\beta 1, \beta 2,$ and $\beta 3$ = Beta coefficients

ε = variance errors component

In the model, β_0 = the constant term while the coefficient $\beta_i = 1 \ldots 3$ were used to measure the sensitivity of the dependent variable (Y) to unit change in the predictor variables X_1, X_2 and X_3. The error (ϵ) term captures the unexplained variations in the model. The results were presented on tables.

.

3.9 Ethical Considerations

The study used a university-stamped letter indicating the purpose and objective of the study to ensure that it met ethical standards as set by university policy and guidelines. Before being given the questionnaire, respondents were asked to verbally consent. The respondents were informed of the study's purpose and nature. For confidentiality reasons, respondent identities such as organization names, individual names, or contacts was be indicated in the questionnaire. Google Forms, an online data collection tool, did not collect any system information, such as the IP addresses of the respondents' computers. The researcher obtained approval from the National Commission for Science, Technology, and Innovation (NACOSTI) and Strathmore University to access the identified respondents in order to collect the necessary data for the study. The study emphasized the importance of confidentiality and stated that the information gathered will be used solely for educational purposes. All research materials were kept in securely locked cabinets. That data may be entered into the Strathmore University database, however, it will be adequately encrypted and password protected. Since respondents' organization names or contacts were not be captured in the questionnaire, only those directly involved with this study will have access to anonymized information. The information was kept confidential and used for academic purposes with the view of improving the adoption of cybersecurity in large manufacturing companies. The information was be used in any way without the respondents' express permission.

3.10 Chapter Summary

This chapter gave an account of the research design and methodology that was used to carry out the study in order to assess the factors influencing adoption of cybersecurity in large manufacturing companies in Nairobi County. The population consisted of large manufacturing companies in Nairobi County, with a sample drawn from Kenya Association of Manufacturers. Data was then analyzed using SPSS. Finally, ethical considerations were observed during the study.

CHAPTER 4: PRESENTATION OF RESEARCH FINDIINGS

4.1 Introduction

This chapter entails data presentation, analysis and interpretation of findings in order to address the study objectives. The primary objective of the study was to analyze the factors that influence the adoption of cybersecurity of large manufacturing companies in Nairobi County. This section presents the results obtained from analysis of the primary data collected using the structured questionnaire.

4.2 Response Rate and General Information of Respondents

4.2.1 Response Rate

This section showed the return rate of the questionnaires distributed to the respondents. This helped to determine whether the number of questionnaires returned (responses) were adequate for data analysis and interpretation of results to continue. The examination focused on the collection of research data from 184 CIOs/CISO/ICT Managers and ICT Officers/Systems Analysts/System Administrators.

The main approaches used in the data collection relied on physical questionnaires and Google forms as survey tools. The sample size was 114 large manufacturing firms. The total sample size of the respondents was therefore 228 of large manufacturing companies within Nairobi County. The study was able to obtain responses from 92 large manufacturing firms. Therefore, the study obtained 184 completed questionnaires, which is an 80.7% response rate, as shown in table 4.1. This was deemed adequate for statistical analysis. Kothari (2013) indicates that a response rate of above 60% of the sample respondents is more than adequate for the generalization of the findings to the overall sample.

Table 4.1: Response rates

Category	Frequency	Percentage
Issued	228	100%
Returned	184	80.70%
Not Returned	44	19.30%

Source: Researcher (2023)

4.2.2 General Information of Respondents

The section below provided information on the various demographic profile information sought from the various participants of the study including their gender, age, number of years in the company, education level, sector of the organization, number of employees, annual revenue and designation in the organization. The findings are summarized in detail in Table 4.2 below.

Table 4.2: Respondents demographic information

		Frequency	Percent
Gender	Male	131	71.12
	Female	53	28.80
Age	21-30 years	36	19.57
	31-40 years	80	43.48
	41-50 years	56	30.98
	51 years and above	12	6.52
Number of years in the company	Less than 1 year	32	17.39
	1 - 3 years	65	35.33
	3 years and above	87	47.28
Education level	Certificate/Diploma	67	36.40
	Degree	99	53.80
	Masters	17	9.24
	PhD	1	0.54
	100 – or less	15	8.15
	101 – 999	93	50.54
	1000 and above	76	41.30
Annual revenue	Less than 1 billion	32	17.39
	1 – 10 billion	86	46.74
	11 – 20 billion	44	23.91
	21 – 50 billion	12	6.52
	Above 50 billion	10	5.43
Role in the organization	Chief Information Officer (CIO)	3	1.63
	ICT Manager/Director	78	42.39
	Chief Information Security Officer	4	2.17
	ICT Officer/Systems Analyst/System Administrator	99	53.8
Sector of the organization	Building, Mining and Construction	4	2.17
	Chemical & Allied	34	18.48
	Energy, Electricals & Electronics	12	6.52
	Food & Beverage	42	22.83
	Leather & Footwear	12	6.52
	Metal & Allied	6	3.26
	Automotive	12	6.52
	Paper & Paperboard	20	10.87
	Pharmaceutical & Medical Equipment	12	6.52
	Textile & Apparels	8	4.35
	Timber, Wood & Furniture	22	11.96

Source: Researcher (2023)

The study looked at the gender of the participants and the results revealed that majority of the respondents were male comprising 71.12% of the total respondents with only 28.88% of the respondents were female. Based on the findings presented in Table 4.2, the responses revealed that the gender distribution among the ICT employees of the Kenyan large manufacturing companies was unequal, specifically, the study found that a higher percentage of the respondents were male (71.12%) than their female (28.88%) counterparts. A significant variance (78) may be a symptom of a gender imbalance in the industry if there is a major underrepresentation of male or female employees in the management ranks of the manufacturing industry. This could impact the general effectiveness and competitiveness of cybersecurity adoption since different leadership philosophies and decision-making processes can result in more innovative and successful decision-making. A gender disparity may also reflect underlying social and cultural issues that limit access to opportunities, networks, and resources. To advance gender equality and provide both women and men the power to have a positive impact on the sector's expansion and development, it may be crucial to address gender gaps in the adoption of cybersecurity. This gender parity may have implications for adoption of cybersecurity. Further analysis and interpretation of the data may be necessary to determine if and how gender influences cybersecurity adoption in this context.

The majority of the respondents 43.48% were aged between 31-40 years while 30.98% were aged between 41-50 years as shown in Table 4.2. Majority of the respondents fall in these two aged brackets which implies that majority of the respondents were aged 31-50 years which is considered as the productive age. According to the statistics, employees over the age of 51 years make up a lesser percentage of the sample. The comparatively smaller presence of older employees shows that these manufacturing companies may have room for succession planning. Accordingly, employees in the age categories of 21–30 years and 31–40 years might be prepared for leadership positions to enable a seamless management transfer when older managers leave employment. Between older and younger employees, there is a chance for knowledge transfer when there is a balanced distribution across the various age groups. While younger employees may have a better grasp of emerging cybersecurity technology, older employees may have important industry experience and knowledge. Utilizing the multiple skill sets and experiences prevalent across different age groups, encouraging information exchange, and offering training programs may increase the adoption of developing cybersecurity technologies.

The findings showed that a majority of the respondents had a tenure of more than one year in their current organizations at the time of filling the questionnaire. This implies that they had the capacity to offer reliable information based on their knowledge and experience in adoption of cybersecurity within the company. Most

of the respondents had a bachelor's degree as the highest education qualification. This suggests that employees with less formal education are less prevalent in the adoption of cybersecurity in large manufacturing companies in Nairobi County. The greater percentage of employees with a degree implies that large manufacturing companies prioritize employing people with specific knowledge and abilities for cybersecurity adoption. This can highlight the significance of cybersecurity skill sets frequently learned through higher education. A greater level of education may be necessary for some jobs and responsibilities to manage complicated operations and decision-making processes, which is consistent with industry norms and the high number of employees with degree credentials.

The findings revealed that 22.83% (n=42) were from Food and Beverage sector, 18.48% (n=34) were from Chemical and Allied, 11.96% (n=22) were from Paper and Paperboard sector, 11.96% (n=22) were from Timber, Wood and Furniture sector, 7.61% (n=14) were from Automotive sector, 6.52% (n=12) were from Energy, Electricals and Electronics sector, 5.43% (n=10) were from Pharmaceutical and Medical equipment sector, 4.89% (n=9) were from Leather and Footwear sector, 4.35% (n=8) were from Textile and Apparel sector, 3.26% were from Metal and Allied sector and 0.54% (n=1) were from Building, Mining and Construction as shown in Table 4.2. This data provides insight into the distribution of different sectors,

The study was interested in the number of employees working within large manufacturing companies, and the results pointed out that in the majority of the institutions, 50.54% (n= 93) had 101-999 employees, 41.30% (n= 76) had 1000 and above employees, and 8.15% of the firms had between 100 or less employees (n= 15). The findings were an indication that manufacturing companies have an adequate workforce that can support the execution of cybersecurity adoption measures in the industry. The research examined the revenue generation capacity of the large manufacturing firms, and the analysis is provided. The results show that most of the manufacturing companies 46.74% (n=86) had an annual turnover of 1-10 billion, 23.91% (n=44) had an annual turnover of 11-20 billion, 17.39% (n=32) of the institutions generated a turnover of less than 1 billion, and 6.52% (n=12) had an annual turnover of 21 – 50 billion, and 5.43% had an annual turnover of over 50 billion Kenya shillings. The analysis highlights that a majority of the companies have adequate financial resources generation capacity which can be critical to enacting cybersecurity adoption measures within the industry.

The study results showed that most of the respondents, 53.80% of the respondents were ICT Officers/Systems Analysts/System Administrators within the large manufacturing companies, 42.40% were ICT Managers/Directors, 2.17% were CISOs, and 1.63% were CIOs. The participants in the study play a central

role in cybersecurity adoption within the firms and were key to understanding how various factors impact adoption of cybersecurity in the industry.

4.3 Descriptive Analysis

Descriptive analysis of the responses emanating from the Likert scale statements was conducted using mainly the standard deviation and the mean values. The findings were presented in this section in line with the variables of the research study (organizational resource factors, management factors, technological factors and adoption of cybersecurity). A Likert scale of 1 to 5 (1 = strongly disagree, 2 = disagree 3 = Neutral, 4 = Agree, 5 = strongly agree) was used and the mean response rate from the respondents calculated.

4.3.1 Descriptive Statistics on Organizational Resource Factors

The first objective was to determine the influence of organizational resource factors on adoption of cybersecurity within large manufacturing companies. The respondents were asked to indicate their levels of agreement/disagreement with statements on organizational resource factors on adoption of cybersecurity and their responses were as shown in Table 4.3.

Table 4.3: Descriptive Analysis on Organizational Resource Factors

	N	Mean	Std Deviation
The organization has adequate personnel with cybersecurity expertise	184	2.6957	2.3591
The organization has adequate skills to implement and support new cybersecurity technologies.	184	2.5109	2.1894
The organization has internal cybersecurity staff. The organization does not rely on cybersecurity solution vendor support	184	2.5272	2.1417
Budget is a major constraint in the acquisition and implementation of new cybersecurity technologies for the organization	184	2.6848	2.4473
High training costs of the cybersecurity team impede internal capacity development in the organization	184	2.1033	1.8679
The organization has in house cybersecurity skills development programs to enhance staff cybersecurity skills	184	3.5598	3.2621
The organization has set up ICT structures with HR strategies that determine the quality of new entrants into the organization	184	2.3804	2.0668
Overall Score		**2.9374**	**2.3335**

Source: Researcher (2023)

The descriptive statistics revealed that most of the respondents confirmed the contributions of organizational resource factors to the adoption of cybersecurity were moderate (Mean=2.937, Standard Deviation=2.3335). The results show that participants fairly agreed that in house cybersecurity development programs, influences the adoption of cybersecurity in organizations (Mean = 3.5598, Standard Deviation = 3.2621). This indicates

the importance of organizations raising cybersecurity awareness among employees. The results also show that respondents disagreed that the organization does not have internal cybersecurity staff as they rely on cybersecurity solution vendor support which is sufficient (Mean = 2.5272, Standard Deviation = 2.1417). This means that manufacturing companies largely rely on vendors in executing their cybersecurity strategies. This points to a weakness in cybersecurity strategies since the manufacturing companies have also indicated a lack of internal cybersecurity capacity building.

Findings revealed disagreement that there is a lack of skills to implement and support new cybersecurity technologies (Mean = 2.5109, Standard Deviation = 2.1894). Additionally, there was a disagreement that the organization has adequate personnel with cybersecurity expertise (Mean = 2.6957, Standard Deviation = 2.3591). This shows that manufacturing companies have a shortage of cybersecurity experts. The results also showed that respondents were not in agreement on whether the management has set up ICT structures with HR strategies that determine the quality of new entrants into the organization (Mean = 2.3804, Standard Deviation = 2.0668). This disagreement implies that several manufacturing companies lack alignment between the ICT structure and the HR strategies for bringing employees onboard. Participants also disagreed on whether high training costs of the cybersecurity team impede internal capacity development (Mean = 2.1033, Standard Deviation = 1.8679). This implies that apart from high training costs for cybersecurity, other factors were also impeding internal cybersecurity skills in manufacturing companies.

4.3.2 Descriptive Statistics on Management Factors

The second objective was to establish the influence of management factors on adoption of cybersecurity within large manufacturing companies. The respondents were asked to indicate their levels of agreement/disagreement with statements on management factors on adoption of cybersecurity and their responses were as shown in Table 4.4.

Table 4.4: Descriptive Analysis on Management Factors

	N	Mean	Std Deviation
The organization management ensures there is a cybersecurity awareness programs that staff are mandated to take part in.	184	2.8967	2.7047
The organization's management board has ICT competencies.	184	2.7880	2.5238
The leadership team in the organization positively influence employees' attitude towards cybersecurity awareness.	184	2.9293	2.6375
The top management ICT competency helps in determining the choice of technologies and tools that the organization adopts and how these are in turn updated over time.	184	3.5217	3.2737

The management has put in place adequate internal ICT/cybersecurity policies which they monitor regularly in the organization.	184	2.6196	2.4227
The organization management assesses the cost of potential cybersecurity breaches to determine the right level of investment to mitigate the risk.	184	2.6033	2.3313
The organization's top management awareness about cyber attacks' success probability, influences higher investment in adoption of cybersecurity.	184	3.4185	3.1347
The organization's top management of your company is committed to ensuring a high level of cybersecurity.	184	2.6196	2.3382
Overall Score		**3.1291**	**2.6708**

Source: Researcher (2023)

The findings showed that the overall mean for management factors was 3.1291 with a standard deviation of 2.6708. This shows that most respondents, on average, confirm that management factors have a higher effect on the adoption of cybersecurity of large manufacturing companies. Respondents of the study agreed that the organization's top management awareness of cyber attacks' success probability, influences higher investment in cybersecurity (Mean = 3.4185, Standard Deviation = 3.1347). This indicates that resource allocation towards cybersecurity is influenced by how informed the management is on how vulnerable the organization is to cyber-attacks. The results also show that participants agreed that top management ICT competency helps in determining the choice of technologies and tools that our organization adopts, and how these were in turn updated over time (Mean = 3.5217, Standard Deviation = 3.2737). This result shows that the technical capacity of the management plays a major role in influencing IT governance and investment in technologies that support the adoption of cybersecurity. The participants also disagreed with the statement that the organization assesses the cost of potential cybersecurity breaches to determine the right level of investment to mitigate the risk (Mean = 2.6033, Standard Deviation = 2.3313). This implies that cybersecurity investment by manufacturing companies is not based on the anticipated cost of potential cybersecurity breaches.

The results show disagreement among respondents that the organization management ensures there are cybersecurity awareness programs that staff is mandated to take part in (Mean = 2.8967, Standard Deviation = 2.7047). This shows that the management in manufacturing companies is to a large extent not influencing the cybersecurity awareness programs in their organizations. The analysis points to disagreement among respondents that management has put in place adequate internal ICT/cybersecurity policies which they

monitor regularly in the organization (Mean = 2.6196, Standard Deviation = 2.4227). This result points to a shortage of cybersecurity skills in manufacturing companies.

4.3.3 Descriptive Statistics on Technological Factors

The third objective was to determine the influence of technological factors on adoption of cybersecurity within large manufacturing companies. The respondents were asked to indicate their levels of agreement/disagreement with statements on technological factors on adoption of cybersecurity and their responses were as shown in Table 4.5.

Table 4.5: Descriptive Analysis on Technological Factors

	N	Mean	Std Deviation
The organization maintains confidentiality of privileged information stored in the organization's critical assets or ICT network	184	2.8859	2.6906
The organization maintains integrity of information stored in the organization's critical assets or ICT networks	184	2.5924	2.4047
The organization maintains availability of information stored in the organization's critical assets or ICT network	184	2.6467	2.4428
The cost of cybersecurity incidences is not clear to the organization hence, affecting uptake of cyber insurance	184	2.8859	2.6085
The organization has set a baseline configuration to guide the setup of cybersecurity infrastructure	184	2.9293	2.7027
The organization cybersecurity technology has simplified steps for users to comprehend	184	3.8533	3.4922
The organization cybersecurity technology is easy to operate in terms of ease of remembering and guidance	184	3.3370	3.0306
The organization cybersecurity infrastructure is efficient, effective and improves performance and productivity	184	2.8043	2.4760
Overall Score		**2.9918**	**2.7310**

Source: Researcher (2023)

The findings revealed that the overall mean for technological factors was 2.9918, with a standard deviation of 2.7310. This shows that most respondents on average, confirm that technological factors have a higher effect on the adoption of cybersecurity of manufacturing companies. Participants agreed that the organization cybersecurity technology has simplified steps for users to comprehend (Mean = 3.8533, Standard Deviation = 3.4922). This indicates that organizations have simplified cybersecurity technologies that were readily understood by users. The analysis showed agreement that the cost of cybersecurity incidences is not clear to

the organization hence affecting uptake of cyber insurance (Mean = 2.8859, Standard Deviation = 2.6085). The analysis showed no consensus among respondents on whether the organization has set a baseline configuration to guide the setup of cybersecurity infrastructure (Mean = 2.9293, Standard Deviation = 2.7027) because they are not aware of the prevention and detection tools. The respondents neither agreed nor disagreed on whether the organization cybersecurity infrastructure is efficient, effective and improves performance and productivity (Mean = 2.8043, Standard Deviation = 2.4760).

4.3.4 Descriptive Statistics on Adoption of Cybersecurity

The dependent variable was adoption of cybersecurity within manufacturing companies. The respondents were required to indicate the level of agreement regarding the adoption of cybersecurity in large manufacturing companies and their responses were as shown in Table 4.6.

Table 4.6: Descriptive Analysis on Adoption of Cybersecurity

	N	Mean	Std Deviation
Threat and vulnerability assessment			
The organization ensures all threats and vulnerabilities identified are mitigated and documented.	184	2.7826	2.5644
The organization classifies and prioritizes different cyber risks facing the institution on its critical assets.	184	2.8098	2.5855
The organization regularly performs cybersecurity assessment exercise.	184	2.8913	2.6355
The organization periodically does drill tests on the business continuity plan to check its adequacy.	184	2.7663	2.5108
The organization has access to threat intelligence reports directly related the organization.	184	2.8478	2.7006
Protection			
The organization has valid user two-factor authentication (login and password).	184	3.8315	3.4891
The organization protection facility has antivirus and firewalls security features.	184	3.4946	3.2454
The organization has adopted services on Virtual Private Network or other remote access capability.	184	3.3641	3.0840
The organization has authentication and encryption for Wi-Fi access.	184	3.8043	3.4484
The organization limits access to logs, change logs and periodically reviews logging policies and procedures	184	3.1033	2.8987
Detection			
The organization detection facility has alerts for threats	184	2.7337	2.4782
The organization detection facility has the capability to check anomalies and report events.	184	2.8207	2.5834
The organization detection facility has inbuilt cybersecurity corrective processes.	184	2.6793	2.4935
The organization detection facility has an inbuilt cybersecurity audit logs reporting system.	184	2.7228	2.5410

The organization has threat intelligence teams that go through internal and external intelligence databases and remove any false positives.	184	2.3696	2.2116
Recovery (Response)			
The organization response facility allows for efficient incidence turnaround time.	184	2.9565	2.7087
The organization has plans in place to ensure business operations continue in the event of an adverse scenario.	184	2.7174	2.5216
The cyber incident response plan for the enterprise is tailored to rapidly contain damages and mobilize response resources if a cyber incident were to occur.	184	2.5054	2.2746
The organization has documented plans for responding to and aid in recovering from cyber incidents that include recovery time objectives and recovery point.	184	2.3587	2.1993
The organization has a documented cybersecurity strategy.	184	2.4783	2.2984
Overall Score		**3.0974**	**2.6736**

Source: Researcher (2023)

Respondents agreed that organizations have valid user two-factor authentication (login and password) (Mean = 3.8315, Standard Deviation = 3.4891). The analysis showed agreement that organizations protection facility have antivirus and firewalls security features (Mean = 3.4946, Standard Deviation = 3.2454). There was no consensus among respondents on whether the organization response facility allows for efficient incidence turnaround time (Mean = 2.9565, Standard Deviation = 2.7087). Further, respondents did not agree on whether the organization has a documented cybersecurity strategy (Mean = 2.4783, Standard Deviation = 2.2984). This points to gaps in addressing redundant services that enable organizations to replace their systems with an alternative when primary services were not available in a cyber crisis.

The findings indicate disagreement among respondents on whether the organization classifies and prioritizes different cyber risks facing the institution on its critical assets (Mean = 2.8098, Standard Deviation = 2.5855). These results indicate that there is a lack of a recognized role for cybersecurity risk in the organization undertaking root cause analysis for cyber crisis to identify the cause of cybersecurity gaps. The low score on lack of documented plans for responding and recovering from cyber incidents (Mean = 2.4783, Standard Deviation = 2.2984) indicates that manufacturing companies have gaps in having recovery teams in place to deal with a cyber crisis quickly for both minor or major cyber incidents.

4.4 Inferential Analysis

Inferential statistics is a field of statistics that deals with inferences, generalizations, estimates, and approximations based on sample data (Mugenda & Mugenda, 2003). Based on information gathered from that target population, it is utilized to make decisions concerning that population. Correlation analysis was

used to apply inferential statistics and determine the nature of the relationship between the dependent variable and the independent variables as well as whether there was statistical significance.

4.4.1 Correlation Analysis Results

Correlation analysis is a statistical method used to determine if there's a significant association between two variables (Shrestha, 2020). This technique is used to determine whether one variable impact another, and to forecast future observations. The strength and direction of this association are measured using a correlation coefficient, typically denoted by the letter 'r'. The correlation coefficient ranges from -1 to 1. A high correlation means that two or more variables have a strong relationship with each other, while a weak correlation means that the variables are hardly related (Jihadi et al., 2021). This analysis is fundamentally based on the assumption of a straight-line linear relationship between the quantitative variables, and it measures the strength or the extent of an association between the variables and also its direction.

This study carried out correlations analysis to assess the nature and the strength of the association between factors influencing the adoption of cybersecurity for large manufacturing companies. Correlation coefficient was computed and used to test whether there existed interdependency between independent variables and also whether the independent variables were associated to the dependent variable. The results for the correlation in the study are as presented on Table 4.7.

Table 4.7: Correlation Matrix

		Adoption of Cybersecurity	Organizational Resource Factors	Management Factors	Technological Factors
Adoption of Cybersecurity	Pearson Correlation	1.000			
	Sig. (2- tailed)	.			
Organizational Resource Factors	Pearson Correlation	.329**	1.000		
	Sig. (2- tailed)	0.000	.		
Management Factors	Pearson Correlation	.477**	.283*	1.000	
	Sig. (2- tailed)	0.000	0.000	.	
Technological Factors	Pearson Correlation	.392**	.401**	0.584**	1.000
	Sig. (2- tailed)	0.000	0.000	0.000	

** Correlation is significant at the 0.01 level (2-tailed).
Source: Researcher (2023)

The correlation analysis performed in the study and presented in Table 4.7 revealed significant associations between adoption of cybersecurity and the factors examined, organizational resource factors, management factors and technological factors. Adoption of cybersecurity was found to have a moderately positive and significant association with organizational resource factors, as denoted by a moderate Pearson correlation coefficient of 0.329. This implies that the higher the level of organizational resource factors implemented by manufacturing companies, the higher the level of adoption of cybersecurity was likely to be. This correlation was statistically significant at the 0.01 level. This is consistent with the findings of Kiganda (2022) which confirmed a moderate positive effect of organizational resource factors on adoption of cybersecurity.

Similarly, management factors had a positive and significant association with adoption of cybersecurity, as indicated by a moderate Pearson correlation coefficient of 0.477. This finding suggests that improvements in management factors were also associated with increased adoption of cybersecurity. This correlation was statistically significant at the 0.01 level.

Moreover, technological factors demonstrated a moderate positive correlation with adoption of cybersecurity, with a moderate Pearson correlation coefficient of 0.392, suggesting that more technological practices were likely associated with higher levels of adoption of cybersecurity. This correlation was statistically significant at the 0.01 level.

Additionally, there were interdependencies found among the independent variables themselves. Organizational resource factors were moderately correlated with both management factors (r = 0.283) and technological factors (r = 401), suggesting that these different factors often went hand-in-hand in adoption of cybersecurity in manufacturing companies. Management factors and technological factors were also moderately correlated (r = 0.584), further supporting the idea of interdependency among the independent variables. In general, the correlations were statistically significant at the 0.01 level, providing moderately strong evidence that these relationships were not due to chance. The results of this study highlight the important role that these factors play in enhancing adoption of cybersecurity within a company.

4.4.1.1 Regression between Organizational Resource Factors and Adoption of Cybersecurity

Regression analysis was carried out in order to establish the relationship between organizational resource factors and adoption of cybersecurity for manufacturing companies. The summary of the regression findings is shown in Table 4.8.

Table 4.8: Regression Summary Organizational Resource Factors and Adoption of Cybersecurity

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.531[a]	.342	.341	4.7794

a. Predictors: (Constant), Organizational Resource Factors
Source: Researcher (2023)

The regression tests showed an extracted R square value of (0. 342). This implies that organizational resource factors explain 34.2% of the change in adoption of cybersecurity with the remaining 65.8% being attributed to other factors not considered in the regression model. Table 4.9 shows analysis of variance results.

Table 4.9: ANOVA Summary Organizational Resource Factors and Adoption of Cybersecurity

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2367.8791	1	2367.8791	7.6989	.000[b]
	Residual	522.4653	60	14.01		
	Total	2890.34	61			

a. Dependent Variable: Adoption of Cybersecurity
b. Predictors: (Constant), Organization Resource Factors
Source: Researcher (2023)

The ANOVA findings presented in Table 4.9, show that the F-statistic value is 7.6989 with a p-value of 0.000. This indicates that; F (1212) = 7.6989, p = 0.000 (p-value < 0.000). This implies that the model used was significant in explaining the relationship between organizational resource factors and adoption of cybersecurity for manufacturing companies. Table 4.10 shows regression coefficient results.

Table 4.10: Regression Coefficient Organizational Resource Factors and Adoption of Cybersecurity

		Unstandardized Coefficients		Standardized Coefficients Beta		
Model		Beta	Std. Error	Beta	t	Sig.
1	(Constant)	1.253	0.007		5.14	0.000
	Organizational Resource Factors	0.514	0.044	0.031	2.274	0.000

a. Dependent Variable: Adoption of Cybersecurity
Source: (Researcher) 2023

$Y = 1.253 + 0.514X_1$

The resulting regression coefficients of the study variables showed a positive and significant relationship between organizational resource factors and adoption of cybersecurity (β=0.514, p-value= 0.000<0.05). This implies that for every unit change in organizational resource factors, there will be an expected 0.514 unit change in adoption of cybersecurity for manufacturing companies in Nairobi County.

4.4.1.2 Regression between Management Factors and Adoption of Cybersecurity

Regression analysis was carried out in order to establish the influence of management factors on adoption of cybersecurity in large manufacturing companies. The summary of the regression findings is shown in Table 4.11.

Table 4.11: Regression Summary Management Factors and Adoption of Cybersecurity

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.731[a]	.485	.484	4.7794

a. Predictors: (Constant), Management Factors
Source: Researcher (2023)

The regression tests showed an extracted R square value of (0.485). This implies that management factors explain 48.5% of the change in adoption of cybersecurity in manufacturing companies with the remaining 51.5% being attributed to other factors not considered in the regression model. Table 4.12 shows analysis of variance results.

Table 4.12: ANOVA Summary Management Factors and Adoption of Cybersecurity

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3017.5194	1	3017.5194	231.1101	.000[b]
	Residual	631.9173	60	4.5493		
	Total	3703.4367	61			

b. Dependent Variable: Adoption of Cybersecurity
c. Predictors: (Constant), Management Factors

Source: Researcher (2023)

The ANOVA findings presented in Table 4.12 show that the F-statistic value is 231.1101 with a p-value of 0.000. This indicates that; F (1212) = 231.1101, p = 0.000 (p-value < 0.000). This implies that the model

used was significant in explaining the relationship between management factors and adoption of cybersecurity for large manufacturing companies. Table 4.13 shows regression coefficient results.

Table 4.13: Regression Coefficient Management Factors and Adoption of Cybersecurity

		Unstandardized Coefficients		Standardized Coefficients Beta		
Model		Beta	Std. Error	Beta	t	Sig.
1	(Constant)	2.197	7.191		0.709	0.33
	Management Factors	0.519	0.004	0.481	2.274	0.000

a. Dependent Variable: Adoption of Cybersecurity
Source: Researcher (2023)
$Y = 2.197 + 0.519X_2$

The resulting regression coefficients of the study variables showed a positive and significant relationship between management factors and adoption of cybersecurity (β=0.481, p-value= 0.000<0.05). This implies that for every unit change in management factors, there will be an expected 0.481-unit change in adoption of cybersecurity for manufacturing companies.

4.4.1.3 Regression between Technological Factors and Adoption of Cybersecurity

Regression analysis was carried out in order to establish the influence of technological factors on adoption of cybersecurity for manufacturing companies. The summary of the regression findings is shown in Table 4.14.

Table 4.14: Regression Summary Technological Factors and Adoption of Cybersecurity

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.391[a]	.280	.279	4.4145

a. Predictors: (Constant), Technological Factors
Source: Researcher (2023)

The regression tests showed an extracted R square value of (0.280). This implies that technological factors explain 28.0% of the change in adoption of cybersecurity for manufacturing companies with the remaining

72% being attributed to other factors not considered in the regression model. Table 4.15 shows analysis of variance results.

Table 4.15: ANOVA Summary Technological Factors and Adoption of Cybersecurity

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	1918.2359	1	1918.2359	144.9161	.000[b]
	Residual	410	60	9.770		
	Total		61			

a. Dependent Variable: Adoption of Cybersecurity
b. Predictors: (Constant), Technological Factors
Source: Researcher (2023)

The ANOVA findings presented in Table 4.15, show that the F-statistic value is 144.9161 with a p-value of 0.000. This indicates that; F (1212) = 144.9161, p = 0.000 (p-value < 0.000). This implies that the model used was significant in explaining the relationship between technological factors and adoption of cybersecurity for manufacturing companies. Table 4.16 shows regression coefficient results.

Table 4.16: Regression Coefficient Technological Factors and Adoption of Cybersecurity

		Unstandardized Coefficients		Standardized Coefficients Beta		
Model		Beta	Std. Error	Beta	t	Sig.
1	(Constant)	1.750	5.021		7.455	0.00
	Technological Factors	0.329	0.17	0.181	18.742	0.000

a. Dependent Variable: Adoption of Cybersecurity
Source: Researcher (2023)

$Y = 1.750 + 0.329X_3$

The resulting regression coefficients of the study variables showed a positive and significant relationship between technological factors and adoption of cybersecurity for manufacturing companies (β=0.329, p-value= 0.000<0.05). This implies that for every unit change in technological factors, there will be an expected 0.329 unit change in adoption of cybersecurity for manufacturing companies.

4.4.1.4 Multiple Linear Regression Analysis Results

Regression analysis is a statistical method that is used to examine the relationship between two or more variables of interest. Regression analyses predict the exact value of the dependent variable for any given value of the independent variable(s), provided that the relationship between these variables is linear. For the case of this study multiple regression analysis was conducted to establish the overall statistical significance and relationship between the factors and adoption of cybersecurity for manufacturing companies. The model summary results are shown in Table 4.17.

Table 4.17: Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.531[a]	.417	.415	0.47794

a. Predictors: (Constant), Organizational Resource Factors, Management Factors, Technological Factors
Source: Researcher (2023)

The results in Table 4.17 shows a coefficient of determination (R^2) of 0.417 which implies that 41.7% of the variance in the dependent variable was explained by the model. This is a high value, indicating a good fit of the model. This coefficient of determination indicates that the independent variables used in this study of organizational resource factors, management factors and technological factors were jointly responsible for 41.7% of the variation in adoption of cybersecurity for manufacturing companies. The adjusted R squared of 0.415 depicts that the same independent variables in exclusion of the constant variable explains the variation in adoption of cybersecurity by 41.5%. The remaining 58.3% of the variation in adoption of cybersecurity for manufacturing companies can be accounted for by other factors which were not part of the current model. In general, the model summary indicates that organizational resource factors, management factors and technological factors are strong predictors of the adoption of cybersecurity for manufacturing companies. These variables collectively explain 41.7% of the variance in the dependent variable, and the model's predictions are estimated to have a standard deviation of 0.47794. Results in Table 4.18 shows analysis of variance results.

Table 4.18: ANOVA

	Model Sum of Squares	Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2367.8791	1	589.23	44.6989	.0010[b]
	Residual	2522.4653	60	14.01		
	Total	4,890.34	61			

c. Dependent Variable: Adoption of Cybersecurity
d. Predictors: (Constant), Organization Resource Factors, Management Factors, Technological Factors
Source: Researcher (2023)

The analysis of variance results in Table 4.18 indicate that the model adopted in this study was statistically significant in explaining the factors (organizational resource factors, management factors and technological factors) influencing adoption of cybersecurity for manufacturing companies as indicated by a p-value of 0.000<0.05. Table 4.19 depicts regression coefficient results.

Table 4.19: Multiple Regression of Coefficients

		Unstandardized Coefficients		Standardized Coefficients		
Model		**Beta**	**Std. Error**	**Beta**	**t**	**Sig.**
1	(Constant)	0.253	9.021		-0.514	0.000
	Organizational Resource	0.514	0.044	0.031	2.274	0.020
	Management Factors	0.441	0.238	0.719	2.14	0.017
	Technological Factors	0.349	0.717	0.045	3.022	0.006

a. Dependent Variable: Adoption of Cybersecurity
Source: Researcher (2023)

The regression model therefore became;

$Y = 0.253 + .514X_1 + .441X_2 + .349X_3 + 9.021$

Where:

Y = Adoption of cybersecurity

$\mathbf{X_1}$ = Organizational resource factors

$\mathbf{X_2}$ = Management factors

$\mathbf{X_3}$ = Technological factors

The results in Table 4.19 depicts the results of a multiple regression analysis examining the relationships between various factors (organizational resource factors, management factors, technological factors) and adoption of cybersecurity. The coefficients, standard errors, standardized coefficients (beta), t-statistics, and significance (p-values) are reported for each independent variable. The results revealed a constant term of 0.253, representing the expected value of adoption of cybersecurity when all the three factors are equal to zero. This implies that if manufacturing companies were not to implement any of the three factors, the model would predict their adoption of cybersecurity value of 0.253.

The findings revealed a positive and significant relationship between organizational resource factors and adoption of cybersecurity (β = .514, p=.000<.05). This suggests that for every one-unit increase in the organizational resource factors by manufacturing companies, there is an expected 0.514-unit increase in adoption of cybersecurity. This was supported by a t-statistic of 2.274 which is greater than the critical t-statistics of 1.75. This indicates that the organizational resource factors have a statistically significant positive impact on adoption of cybersecurity for manufacturing companies. These findings suggest that enhancing organizational resource factors can lead to improved adoption of cybersecurity, underlining the crucial role of organizational resource factors in driving adoption of cybersecurity in the context of the manufacturing companies analyzed.

Secondly, the study findings revealed that there existed a positive and significant relationship between management factors and adoption of cybersecurity (β =.441, p=.001<.05). The t-statistic is 2.14>1.75. This suggests that for every one-unit increase in the management factors in manufacturing companies, there is an expected 0.441-unit increase in adoption of cybersecurity. This implies that the management factors have a statistically significant positive impact on adoption of cybersecurity for manufacturing companies. The findings imply that increases in management factors are associated with increases in adoption of cybersecurity for manufacturing companies.

Finally, the study found a positive and significant relationship between technological factors and adoption of cybersecurity (β =.349, p=.000<.05). This suggests that for every one-unit increase in the technological factors, there is a 0.349-unit expected increase in adoption of cybersecurity. The t-statistic is 3.022>1.75, implying that the technological factors have a statistically significant positive impact on adoption of cybersecurity. In conclusion, the multiple regression results suggest that all three factors have a statistically significant positive impact on adoption of cybersecurity in manufacturing companies.

4.5 Chapter Summary

The fourth chapter focused on a presentation of the research findings, which revealed the examination was able to obtain 80.7% response rate. 42% of the research responses were obtained from the ICT managers of the manufacturing companies thus underpinning the relevancy of the information provided in analyzing how various factors influence adoption of cybersecurity. The study revealed that most of the participants, 51% had at least 101-999 employees. The correlation analysis showed that organizational resource factors, management factors and technological factors positively influenced the adoption of cybersecurity in manufacturing companies in Nairobi County. The regression established that at least 41.7% of the changes in adoption of cybersecurity within large manufacturing companies were determined by organizational resource factors, management factors and technological factors.

CHAPTER 5: DISCUSSION, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter gives a summary of the major findings, conclusions and recommendations. A discussion of the study's limitations follows before suggestions are provided for future researchers.

5.2 Discussion of the Findings

This section provides discussion of the findings in light of the specific objectives of the study.

5.2.1 Organizational Resource Factors and Adoption of Cybersecurity

The first objective sought the effect of organizational resource factors on the adoption of cybersecurity in large manufacturing firms in Nairobi County. The analysis showed that organizational resource factors have a significant effect on adoption of cybersecurity within large manufacturing companies in Nairobi County. This is in accordance with the Human, Organization and Technology theory which avers that the resources accrued by an organization affect the degree of investment and execution of cybersecurity practices within the organization. General deterrence theory provides a means for analyzing the continuous defense measures to be employed and directing the investments to the most impactful defense measures. The study revealed that changing organizational resource factors significantly contribute to an improvement in adoption of cybersecurity by a factor of .342. These sentiments were also reported in the study by Catota et al. (2018), which found evidence that the quality of resources under control by an organization has a significant influence on the degree of a firm's adoption of cybersecurity.

Similarly, Bagheri (2020) study sought expert opinion and ascertained that the skills and competencies of the cybersecurity team, the degree of investment in technologies, and the frequency of cybersecurity training influence how secure firms will be. The study ascertained that managers must allocate adequate financial resources to gain the technical capacity necessary to guarantee cybersecurity. These findings were also reported by Lykou et al. (2019), who researched threat mitigation and cyber resilience controls in smart airports and determined that good technical practices, good organizational practices, and effective policies and standards are among the main drivers of organizational cyber resilience.

The study by Sallos et al. (2019) also found that firms that possess a unique set of heterogeneous and diversified resources and are supported by competent leadership are in a better position to reconfigure these resources to address cybersecurity challenges. In the study by Kasanga (2021), organizational recruitment strategies determine the technical capacity of an organization's workforce, which is essential to facilitating continuous learning and innovation, effective deployment of heterogeneous resources, and enhanced

cybersecurity. Akech et al. (2020) studied cyber resilience factors within county governments in Kenya and showed that the technical competence of IT staff, financial resources allocated towards cybersecurity, compliance requirements, and management support were all factors of adoption of cybersecurity. Cybersecurity is guaranteed by an organization's access to qualified IT technical cybersecurity specialists who can make industry assessments and formulate effective cybersecurity strategies.

5.2.2 Management Factors and Adoption of Cybersecurity

The second objective sought the effect of management factors on the adoption of cybersecurity in manufacturing companies in Nairobi County. The analysis determined that the support of the management has a significant positive effect on organizations' adoption of cybersecurity. Managers play a key role in cybersecurity development in organizations. This is because fostering a cybersecurity culture, improving employees' workplace satisfaction and designing cybersecurity strategies are usually initiated by managers (Pearlson 2019).

This is in accordance with the Human, Organization and Technology theory which avers that firms with leaders who have a clear understanding of cyber threats will support their organizations towards adoption of cybersecurity. The analysis revealed that resource allocation towards adoption of cybersecurity is influenced by how informed the management is on the vulnerability of the organization to cyber-attacks. Investment in security should be justified by the prevention of substantially higher but ultimately unpredictable losses from security incidents. Hence, decision makers must have a clear understanding of the benefits, problems, and challenges of a cybersecurity solution before endorsing their adoption in practice.

This is in line with the General deterrence theory which provides a means or strategies for managers to allocate resources in the ever-changing cyberspace, including the managers' support in implementing strategies aimed at ensuring manufacturing firms adopt cybersecurity. The study revealed that changing management support significantly contributes to an improvement in adoption of cybersecurity by a factor of .485. These findings collaborated in the study by Lykou et al. (2019), which ascertained that managers play a key role in developing a structural and procedural basis that can enhance continuous intra-and inter-organizational cybersecurity analysis, managing interdisciplinary cyber-risk analysis teams, developing and maintaining a portfolio of cyber-threat scenarios, and creating consistency and synergy in safety and security. Similarly, Jensen (2015) studied adoption of cybersecurity in the maritime industry and determined that maritime managers are essential in developing a set of best practices and guidelines that can direct adoption of cybersecurity and orient long-term goals with global cybersecurity standards.

In Ghana, Affum (2019) investigated organizational cybersecurity in foreign banks and ascertained that managerial support is essential to creating communication systems. The research determined that the ability to maintain voice and data communication always is critical to facilitating threat assessment and response. The study showed that communication improves coordination capability, which influences the level of cooperation between a wide range of security agencies and facilitates cybersecurity. Furthermore, according to Hausken (2020), managers are essential determinants of a company's ability to predict and analyze future threats. The analysis showed that the management's commitment to cybersecurity could be determined by the number of resources allocated towards ensuring organizational cybersecurity measures.

Matern et al. (2019) studied the role of managers in facilitating cybersecurity in public administration and reported similar findings, showing that managers play a key role in selecting human resource strategies that direct recruitment, set corporate ICT structure, and determine the degree to which employees receive infrastructural and cultural support. Top leadership support was determined to be the driving force behind institutional change and increased awareness regarding cybersecurity practices, and instituting changes to address the retention of employees with the required skills. Balakrishnan et al. (2018) found that managers shape cybersecurity strategies and can influence monitoring and detection procedures, cybersecurity culture, communication and coordination, and recovery planning. However, the researchers determined that the managers' aversiveness towards risk influences the organizational approach towards adoption of cybersecurity measures.

5.2.3 Technological Factors and Adoption of Cybersecurity

The third objective of the study was to examine the effect of technological factors on the adoption of cybersecurity with manufacturing firms in Nairobi County. The analysis showed the positive and significant effect of technological factors on the adoption cybersecurity within manufacturing companies. Organizations enhance their cybersecurity practices by following principles-based cybersecurity policies with regular updates as well as adopting change management and flexible approaches with established rules during recovery time. The establishment of cybersecurity policies occurs both before and after cyber crisis, since these policies are updated across the post-incident stage (Denyer, 2017). According to the study by Kumar et al. (2021), the type of technologies used by an organization determines its level of cybersecurity. The study also showed positive relationships between adherence to information security standards and organizational resilience and adoption of cybersecurity.

To counter these cyberattacks, following the soundest practices for online security, such as utilizing strong passwords, avoiding emails from suspicious parties, and keeping the software and operating systems up-to-date is essential. In addition, organizations should implement cybersecurity criteria, such as firewalls, antivirus software, and intrusion detection systems to protect their networks and data from any cyber-attack. With the rise of cyber threats in the digital world, it is essential for both individuals and organizations to take preventative measures against cyber-attacks and malware. This can be accomplished by keeping up-to-date with the most recent dangers and employing efficient cybersecurity measures while devising appropriate strategies to thwart them.

5.3 Conclusions

The factors under investigation have a significant and positive impact on adoption of cybersecurity in manufacturing companies. Below is the conclusion of the study.

Firstly, it is evident that there is a significant positive relationship between organizational resource factors and adoption of cybersecurity measures implying that manufacturing companies should direct sufficient financial and human resources towards meeting the cybersecurity teams budgetary demands as budgetary constraints were affirmed to have an impact on the effective adoption of cybersecurity solutions. Secondly, management factors have a significant positive effect on organizational adoption of cybersecurity measures. This implies that it would be paramount for organizations seeking to adopt cybersecurity measures to hire managers who are conscious of cyber threats to ensure that they provide competent technical and financial support and redirect organizational efforts towards meeting cybersecurity requirements.

Thirdly, technological factors have a significant positive effect on the adoption of cybersecurity in manufacturing companies. The study determined that the quality of technological infrastructure that already exists in the organization has a significant impact on an organization's ability to successfully integrate emerging cyber technologies into the security setup and meet cybersecurity goals. In conclusion, there is evidence that an organization that can effectively manage its resources, harness the management support and technological advancement can be able to improve the organization's adoption of cybersecurity.

5.4 Recommendations

5.4.1 Policy Recommendations

Policy makers should take into account the investment of infrastructure to maintain cybersecurity of the internet-based technologies that have been adopted by most large manufacturing companies. Policymakers

should also prepare the cultivated and skillful manpower who will implement the preventive measures to secure assets, technology and manufacturing facilities against cyberthreats.

Through the process of policy makers lobbying other stakeholders, cybersecurity awareness can be made more prominent so that cybersecurity is placed in the context of community responsiveness. What policy makers also need to note is that responsibility for safeguarding infrastructure needs to be viewed as a shared responsibility. The interdependence of network systems warrants that stakeholders provide and maintain a level of service that, if disrupted during a successful attack, requires emergency action to restore the situation. Policy makers should recognize that the elimination of cyber-attacks and the reduction of uncertainty should be viewed as a shared responsibility between government and industry. This would encourage firms to invest in training and awareness programs for employees to adhere to cybersecurity regulations and engage with regulators, policy makers and industry associations to keep updated on evolving threats and best practices.

The study will also benefit policy makers on the areas of the cybersecurity adoption that require policy interventions for the purpose of providing an efficient cybersecurity measure. Internal and external policy makers may be informed on the role of cybersecurity optimization on the performance of manufacturing firms in Kenya hence they may be more informed when making policy touching in this sector. Their findings can provide cybersecurity policy makers a way to quantify the judgments of their technical team regarding cybersecurity policy.

5.4.2 Managerial Recommendations

The study recommends that managements take a central role in promoting the firm's cybersecurity adoption. Managers should be directly involved in formulating cybersecurity strategies, selecting cybersecurity programs, and allocating resources. The study also recommends that managers align cybersecurity decisions with organizational goals and capabilities to reduce organizational misalignment, which can affect effective adoption of cybersecurity measures. The degree of management support determines how secure the organizations will be from cyber threats. The study recommends that to adopt cybersecurity measures, the management must be ready to allocate significant resources, to ensure that they meet the high costs associated with pursuing adoption of cybersecurity measures. Significant investments must be made by managers to acquire the technologies and competence necessary to ensure they meet internationally recognized cybersecurity standards.

5.4.3 Theoretical Recommendations

This study contributes to Human, Organization and Technological theory by providing empirical evidence of the impact of factors influencing adoption of cybersecurity which affirms that a firm's resources have a significant impact on its ability to realize organizational goals, in this case adopting cybersecurity measures. The framework propagates that the more technology, human and organization fit with each other, the higher the potential of adoption of technology. The study's findings add to the body of knowledge because it is a multilevel model that incorporates the technological factors, organizational resource factors and management factors influencing the adoption of cybersecurity measures. This study also addressed a gap in the literature by conducting research into adoption of cybersecurity that considered more than the recovery aspect. It also confirmed those previously identified in past studies. By investigating the existing literature on non-technical factors of adoption of cybersecurity, this research provided additional insights into how those factors in manufacturing companies can drive and potentially influence the adoption of cybersecurity in companies.

5.5 Study Limitations and Suggestions for Further

One of the limitations of this study was that the research focused on large manufacturing companies in Nairobi County hence more in-depth research can be conducted focusing on the entire manufacturing sector in Kenya. Future studies could also explore adoption of cybersecurity in other industries such as the healthcare sector which is highly reliant on cybersecurity for effectiveness. The study found organizational resource, management and technological factors influence 41.7% of adoption of cybersecurity. Therefore, the need to study the other factors not accounted for in the study is necessary. To help confirm the results from this study, future research could potentially consider the analysis of the data using another qualitative analysis method to investigate whether similar patterns of themes and concepts are achieved. The Kenyan findings can also be compared to investigations in other countries. This study's respondents were ICT staff hence, future research on cybersecurity should also incorporate the end-users who are the non-ICT staff to understand their contribution to a firm's adoption of cybersecurity.

5.6 Chapter Summary

This chapter presented the conclusion of this research. The collated findings were discussed, together with the study's contribution to both research and practice. Limitations of the study were presented, with suggestions for future research.

REFERENCES

Abdalla, M., Arshad, Y. Bin, Jarrah, M., & Abu-Khadrah, A. (2021). Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia. *International Journal of Advanced Computer Science and Applications*, *12*(11), 804–810. https://doi.org/10.14569/IJACSA.2021.0121191

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), 123–138. https://doi.org/10.3390/network2010009

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

AL-Hawamleh, A. M. (2023). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures. *International Journal of Advanced Computer Science and Applications*, *14*(2), 801–809. https://doi.org/10.14569/IJACSA.2023.0140292

Aman, W., & Shukaili, J. Al. (2021). A Classification Of Essential Factors For The Development And Implementation Of Cyber Securitym Strategy In Public Sector Organizations. *International Journal of Advanced Computer Science and Applications*, *12*(8), 169–176. https://doi.org/10.14569/IJACSA.2021.0120820

Andronache, A. (2021). Increasing security awareness through lenses of cybersecurity culture. *Journal of Information Systems & Operations Management*, *15.1*(July), 7–23.

Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Aoyama, T., Naruoka, H., Koshijima, I., & Watanabe, K. (2015). How management goes wrong ? – The human factor lessons learned from a cyber incident handling exercise. *Procedia Manufacturing*, *3*(Ahfe), 1082–1087. https://doi.org/10.1016/j.promfg.2015.07.178

Asiltürk, A. (2022). *The Role of Top Management and IT Team Interaction on The Success of Cyber Security Strategies* (Issue March). https://www.researchgate.net/publication/359284842

Awan, J. H., Memon, S., Khan, R. A., Noonari, A. Q., Hussain, Z., & Usman, M. (2017). Security strategies to overcome cyber measures, factors and barriers. *Engineering Science and Technology International Research Journal*, *1*(1), 51–58.

Bada, M., Sasse, A., & Bada, M., Sasse, A., Nurse, J. (2014). Cyber Security Awareness Campaigns: Why They Fail to Change Behavior. *International Conference on Cyber Security for Sustainable Society*, *July*, 38. http://www.cs.ox.ac.uk/publications/publication9343-abstract.html%0Ahttp://discovery.ucl.ac.uk/1468954/1/Awareness CampaignsDraftWorkingPaper.pdf

Badi, S. (2023). *Cybersecurity effectiveness in UK construction firms : an extended McKinsey 7S model approach*. *May*. https://doi.org/10.1108/ECAM-12-2022-1131

Bagheri, S. (2020). Investigating Organisational Aspects of Cyber Resilience in Large Organisations. *University of Tasmania, November 2020*.

Banga, K., & Willem, D. (2018). *HOW TO GROW MANUFACTURING AND CREATE JOBS IN A DIGITAL 10 policy priorities for Kenya*. *November*.

Barth, S., de Jong, M. D. T., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. *Telematics and Informatics*, *68*(February), 101782. https://doi.org/10.1016/j.tele.2022.101782

Bendiek, A., & Metzger, T. (2015). Deterrence theory in the cyber-century. Lessons from a state-of-the-art literature review. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *246*, 553–570.

Bouwens, C. L., & Stafford, R. B. (2019). The role of organizational resilience across the cyber attack lifecycle. *2019 International Annual Conference Proceedings of the American Society for Engineering Management and 40th Meeting Celebration: A Systems Approach to Engineering Management Solutions, ASEM 2019*, 2019.

Cebula, J. J., & Young, L. R. (2010). *A Taxonomy of Operational Cyber Security Risks CERT ® Program A Taxonomy of Operational Cyber Security Risks The original document contains color images*. *December*. http://www.sei.cmu.edu

Chege, L. W. (2018). *Strategic Leadership Teams,board Diversity and Performance of Kenya Association of Manufacturers*.

Cheong, W., Hong, H., Chi, C., Liu, J., & Zhang, Y. (2023). The influence of social education level on cybersecurity awareness and behaviour : a comparative study of university students and working graduates. In *Education and Information Technologies*. Springer US. https://doi.org/10.1007/s10639-022-11121-5

Chizanga, M. K., Agola, J., & Rodrigues, A. (2022). Factors Affecting Cyber Security Awareness in Combating Cyber Crime in Kenyan Public Universities. *International Research Journal of Innovations in Engineering and Technology*, *06*(01), 54–57. https://doi.org/10.47001/irjiet/2022.601011

Choejey, P., Murray, D., & Che Fung, C. (2016). *Exploring Critical Success Factors for Cybersecurity in Bhutan's Government Organizations*. 49–61. https://doi.org/10.5121/csit.2016.61505

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers and Security*, *113*, 102551. https://doi.org/10.1016/j.cose.2021.102551

Cook, K. D. (2017). Effective Cyber Security Strategies for Small Businesses This is to certify that the doctoral study by. *ProQuest Dissertations and Theses, D.B.A.*, 185.

Dalal, R. S., Howard, D. J., Brummel, B. J., & Bennett, R. J. (2022). *Organizational science and cybersecurity : abundant opportunities for research at the interface*. 1–29.

Davies, P. (2017). Northumbria Research Link (www.northumbria.ac.uk/nrl). *Academy of Management*, *51*(September), 1–51.

de Vries, J. (2017). *What drives cyber security investment? Organizational factors and perspectives from decision-makers*. 28.

Doche, C., Selby, J., Selvadurai, R., & Jones, T. (2019). *Submission on Cyber Security Strategy 2020*.

Dunn Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, *30*(7), 1330–1352. https://doi.org/10.1080/13501763.2023.2173274

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), 1–17. https://doi.org/10.1093/cybsec/tyz013

Ehrari, H., Ulrich, F., & Andersen, H. B. (2020). Concerns and trade-offs in information technology acceptance: the balance between the requirement for privacy and the desire for safety. *Communications of the Association for Information Systems*, *47*, 227–247. https://doi.org/10.17705/1CAIS.04716

Eian, I. C., Yong, L. K., Li, M. Y. X., Qi, Y. H., & Fatima, Z. (2020). Cyber Attacks in the Era of Covid-19 and Possible Solution Domains. *Preprints 2020, September*, 1–15. https://doi.org/10.20944/preprints202009.0630.v1

Evaluat, A., Mar, A., & Tech, P. (2023). *AN EVALUATION OF STUDENTS ' CYBERSECURITY*. *7*(1), 78–89. https://doi.org/10.46519/ij3dptdi.1236264

Farheen Ansari, M. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy. *International Research Journal of Engineering and Technology (IRJET)*, *9*(4), 1–6. www.irjet.net

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*(June), 102916. https://doi.org/10.1016/j.jisa.2021.102916

Gao, Y., Zhao, J., Qin, C., Yuan, Q., Zhu, J., Sun, Y., Lu, C., Federal, U., Cear, D. O., Ci, C. D. E., Agr, N., Ci, E. M., Alimentos, T. D. E., Lopes, S., Oliveira, G. O. D. E., Afifah, I., & Sopiany, H. M., Psicologia, P. D. E. P. E. M., Orrico Junior, M., Santos, H. D. S., … Augusto, K. V. O. N. Z. (2023). No Title. *Aleph*, *87*(1,2), 149–200. https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/167638/341506.pdf?sequence=1&isAllowed=y%0Ahttps://repositorio.ufsm.br/bitstream/handle/1/8314/LOEBLEIN%2C LUCINEIA CARLA.pdf?sequence=1&isAllowed=y%0Ahttps://antigo.mdr.gov.br/saneamento/proees

Garba, A. A., & Bade, A. M. (2021). The Current State of Cybersecurity Readiness in Nigeria organizations. *Educational Research (IJMCER)*, *3*(1), 154–162. www.ijmcer.com

Garba, A. A., Siraj, M. M., & Othman, S. H. (2022). An assessment of cybersecurity awareness level among Northeastern University students in Nigeria. *International Journal of Electrical and Computer Engineering*, *12*(1), 572–584. https://doi.org/10.11591/ijece.v12i1.pp572-584

Garba, A., Musa, M. A., & Othman, S. H. (2020). *A Study on Cybersecurity Awareness Among Students in Yobe : A Quantitative*. *11*(July), 41–49.

Geil, A., Sagers, G., Spaulding, A. D., & Wolf, J. R. (2018). Cyber security on the farm: An assessment of cyber security practices in the United States agriculture industry. *International Food and Agribusiness Management Review*, *21*(3), 317–334. https://doi.org/10.22434/IFAMR2017.0045

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A Cyber-Security Culture Framework for Assessing Organization Readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. https://doi.org/10.1080/08874417.2020.1845583

Ghelani, D. (2022). X(X): XX-XX Diptiben Ghelani. Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *American Journal of Science, Engineering and Technology*, *3*(6), 12–19. https://doi.org/10.11648/j.XXXX.2022XXXX.XX

Glory, E.-A., Gordon, S., Kittinger, R., Lakkaraju, K., & McCann, I. (2017). *Tailoring of cyber security technology adoption practices for operational adoption in complex organizations. June*. http://www.osti.gov/servlets/purl/1596209/

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the copenhagen school. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hejase, H. J., Fayyad-Kazan, H. F., Hejase, A. J., & Moukadem, I. A. (2021). Cyber Security amid COVID-19. *Computer and Information Science*, *14*(2), 10. https://doi.org/10.5539/cis.v14n2p10

Jalali, M. S., Razak, S., Gordon, W., Perakslis, E., & Madnick, S. (n.d.). *Health Care and Cybersecurity : Bibliometric Analysis of the Literature Corresponding Author : 21*. https://doi.org/10.2196/12644

Johnston, A. C. (2022). A closer look at organizational cybersecurity research trending topics and limitations. *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(2), 124–133. https://doi.org/10.1108/ocj-07-2022-0013

Justin, C. A., Selvan, A., & Fonceca, C. M. (2023). *Cyber security culture in an IT company : An empirical study Cyber security culture in an IT company : An empirical study*. *April*.

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269–282. https://doi.org/10.1080/10919392.2018.1484598

Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security*, *14*(02), 136–151. https://doi.org/10.4236/jis.2023.142009

Kannus, K., & Ilvonen, I. (2018). Future prospects of cyber security in manufacturing: Findings from a Delphi study. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2018-Janua*, 4762–4771. https://doi.org/10.24251/hicss.2018.599

Kayode, A. B., Arome, G. J., Tolulope, A., & Ajoke, A. O. (2016). Cost-benefit analysis of cyber-security systems. *Lecture Notes in Engineering and Computer Science*, *2225*, 136–144.

Kennison, S. M., & Chan-Tin, E. (2020). Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. *Frontiers in Psychology*, *11*(November). https://doi.org/10.3389/fpsyg.2020.546546

Kent, C., Tanner, M., & Kabanda, S. (2016). How South African SMEs address cyber security: The case of web server logs and intrusion detection. *2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies, EmergiTech 2016*, 100–105. https://doi.org/10.1109/EmergiTech.2016.7737319

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. *Journal of Management Information Systems*, *34*(1), 141–176. https://doi.org/10.1080/07421222.2017.1297173

Kiganda, M. (2022). *An Assessment of the factors affecting cyber resilience in microfinance institutions*.

Kilani, Y. (2020). Cyber-security effect on organizational internal process: Mediating role of technological infrastructure. *Problems and Perspectives in Management*, *18*(1), 449–460. https://doi.org/10.21511/ppm.18(1).2020.39

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber security awareness and education in SA. *South African Computer Journal*, *52*(52), 29–41. https://doi.org/10.18489/sacj.v52i0.201

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240

Lavicza, Z., Fenyvesi, K., Lieban, D., Park, H., Hohenwarter, M., Mantecon, J. D., & Prodromou, T. (2021). This is a self-archived version of an original article . This version may differ from the original in pagination and typographic details. *Business and Society*, *60*(2), 420–453.

Linkov, I., & Palma-Oliveira, J. M. (2017). Resilience and Risk: Methods and Application in Environment, Cyber and Social Domains. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. PartF1, Issue August). https://doi.org/10.1007/978-94-024-1123-2

Lobato, L. C. (2016). *Unraveling the cyber security market : The struggles among cyber security companies and the production of cyber (in)security*. *June*.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2019). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors (Switzerland)*, *19*(1). https://doi.org/10.3390/s19010019

Mangano, F. E. (2018). Modernization of Manufacturing with Cybersecurity at the Forefront. *Thesis Masters*.

Manns, G. (2021). The Adoption of Cybersecurity in Small- to Medium-Sized Businesses: A Correlation Study. *ProQuest Dissertations and Theses*, *May*, 119.

Mijwil, M. M. (2023). The Purpose of Cybersecurity Governance in the Digital Transformation of Public Services and Protecting the Digital Environment. *Mesopotamian Journal of Cyber Security*, *2023*, 1–6. https://doi.org/10.58496/mjcs/2023/001

Miron, W., & Muita, K. (2014). Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review*, *4*(10), 33–39. https://doi.org/10.22215/timreview837

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 1–35. https://doi.org/10.3390/s22020538

Model, C. U., & Alhalafi, N. (2023). *smart cities Exploring the Challenges and Issues in Adopting Cybersecurity in Saudi Smart Cities : Conceptualization of the*. 1523–1544.

Mose, T. (2019). Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives : A case study of Nairobi county. *International Academic Journal of Information Systems and Technology*, *2*(1), 157–182.

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime. *International Journal of Research in Business and Social Science (2147- 4478)*, *11*(4), 384–396. https://doi.org/10.20525/ijrbs.v11i4.1714

Muhati, E. (2018). *Factors affecting cyber-security in Kenya – A Case of Small Medium Enterprises*.

Mullet, V., Sondi, P., & Ramat, E. (2021). A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0. *IEEE Access*, *9*, 23235–23263. https://doi.org/10.1109/ACCESS.2021.3056650

Mupila, F. K. (2023). *An Empirical Study on Cyber Crimes and Cybersecurity Awareness*. 1–24.

Mutunhu, B., Dube, S., Ncube, N., & ... (2022). Cyber Security Awareness and Education Framework for Zimbabwe Universities: A Case of National University of Science and Technology. *Proceedings of the …*, 5–7. https://ieomsociety.org/proceedings/2022nigeria/111.pdf

Mwangi, G. M., & Gitau, R. (2022). Effect of Custom Duty Incentives on Financial Performance of Manufacturing Companies in Kenya. *European Journal of Economic and Financial Research*, *6*(4), 94–104. https://doi.org/10.46827/ejefr.v6i4.1366

Mwaniki, Z., Nyang'au, S., & Ngugi, P. (2022). Relationship Between Entrepreneurial Team and Growth of Small and Medium Manufacturing Enterprises in Kenya. *International Journal of Entrepreneurship and Project Management*, *7*(1), 1–13. https://doi.org/10.47604/ijepm.1490

Naik, L. B. (2022). Cyber Security Challenges and Its Emergning Trends on Latest Technologies. *Interantional Journal of Scientific Research in Engineering and Management*, *06*(06). https://doi.org/10.55041/ijsrem14488

Neri, M., Niccolini, F., & Martino, L. (2023). *Organizational cybersecurity readiness in the ICT sector : a quanti-qualitative assessment readiness*. https://doi.org/10.1108/ICS-05-2023-0084

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). *Influence of Human Factors on Cyber Security within Healthcare Organisations : A Systematic Review*. 1–25.

Nikel, F. H., & Amaechi, A. O. (2022). *An Assessment of Employee Knowledge , Awareness , Attitude towards Organizational Cybersecurity in Cameroon*. *7*(1), 1–11. https://doi.org/10.5539/nct.v7n1p1

Njenga, K., & Jordaan, P. (2016). We Want To Do It Our Way : The Neutralization Approach to Managing Information Systems Security by Small Businesses. *The African Journal of Information Systems*, *8*(1), 42–64.

Noparumpa, T., Ruangkanjanases, A., & Hariguna, T. (2021). *Organization Benefit as an Outcome of Organizational Security Adoption : The Role of Cyber Security Readiness and Technology Readiness*.

NYAWANGA, J. O. (2005). *Meeting the Challenge of Cyber Threats in Emerging Electronic Transaction Technologies in Kenyan Banking Sector*. 74. https://www.uonbi.ac.ke/

Okereafor, K. (2020). *Impacts Of Cyber Attacks On Corporate Business Continuity : Fostering Cyber Impacts Of Cyber Attacks On Corporate Business Continuity : Fostering Cyber Security Consciousness In The Citizenry By Kenneth U . Okereafor , BSc , MSc , MCPN , MNCS , MNIM A Pre*. *March*, 1–31.

Oltramari, A., Hoffman, B., Holistic, A. T., & Risk, C. (2015). *Towards a Human Factors Ontology for Cyber Security*. 26–33.

Opoku-ahene, A. R. (2022). *The Influence of Cyber Security Implementation Strategy on Organizational Knowledge Management and Performance – A Case Study of Sinapi Aba Savings and Loans in Ghana*. 217–228.

Otieno, D. O. (2018). *Cyber security challenges : The Case of Developing Countries*.

Pavel, R. (2021). *Enabling Cybersecurity for the Digital Manufacturing Supply Chain*. 1–63.

Peursum, L. (2015). *Building blocks for a cyber security strategy*. 1–178.

Plessis, A. G. (2021). *Cybersecurity and governance framework of information systems in the South African mining industry*. *November*. https://uir.unisa.ac.za/handle/10500/28935

Prasetio, E. A., & Nurliyana, C. (2023). Evaluating perceived safety of autonomous vehicle : The in fl uence of privacy and cybersecurity to cognitive and emotional safety. *IATSS Research*, *47*(2), 160–170. https://doi.org/10.1016/j.iatssr.2023.06.001

Rawindaran, N., Jayal, A., & Prakash, E. (2021). Machine learning cybersecurity adoption in small and medium enterprises in developed countries. *Computers*, *10*(11). https://doi.org/10.3390/computers10110150

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, *27*(2), 17.

Rokkas, T., & Neokosmidis, I. (2020). Factors affecting the market adoption of cyber-security products in energy and electrical systems: The case of SPEAR. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3407023.3409315

Rowe, B. R., & Gallaher, M. P. (2006). Private Sector Cyber Security Investment Strategies: An Empirical Analysis. *The Fifth Workshop on the Economics of Information Security (WEIS06)*, 1–23.

Rufai, A., Modi, S., & Wadata, B. (2020). *A Survey of Cyber-Security Practices in Nigeria*. *5*(3), 222–226.

Sallos, M. P., Garcia-perez, A., Bedford, D., & Orlando, B. (2019). *Strategy and organisational cybersecurity : a knowledge-problem perspective*. *20*(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*(2). https://doi.org/10.15394/jdfsl.2017.1476

Senarak, C. (2021a). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *Asian Journal of Shipping and Logistics*, *37*(4), 345–360. https://doi.org/10.1016/j.ajsl.2021.10.002

Senarak, C. (2021b). Port cybersecurity and threat: A structural model for prevention and policy development. *Asian Journal of Shipping and Logistics*, *37*(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001

Shojaifar, A. (2020). *SMEs Confidentiality Issues and Adoption of Good Cybersecurity Practices*. 1–9. http://arxiv.org/abs/2007.08201

Shreeve, B., Gralha, C., Rashid, A., Araujo, J., & Goulão, M. (2022). Making sense of the unknown: How managers make cyber security decisions. *ACM Transactions on Software Engineering and Methodology*. https://doi.org/10.1145/3548682

Trim, P., & Lee, Y.-I. (2022). Strategic Cyber Security Management and Strategic Intelligence. In *Strategic Cyber Security Management*. https://doi.org/10.4324/9781003244295-4

Turk, Ž., García de Soto, B., Mantha, B. R. K., Maciel, A., & Georgescu, A. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction*, *133*. https://doi.org/10.1016/j.autcon.2021.103988

Van Vuuren, J. J., Leenen, L., Phahlamohlaka, J., & Zaaiman, J. (2014). An approach to governance of cybersecurity in South Africa. *Cyber Behavior: Concepts, Methodologies, Tools, and Applications*, *3–4*, 1583–1597. https://doi.org/10.4018/978-1-4666-5942-1.ch082

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, C. N., Yang, F. C., Vo, N. T. M., & Nguyen, V. T. T. (2022). Wireless Communications for Data Security: Efficiency Assessment of Cybersecurity Industry—A Promising Application for UAVs. *Drones*, *6*(11). https://doi.org/10.3390/drones6110363

Weber, K., & Kleine, N. (2020). Chapter 7: Cybersecurity in Health Care. In *The Ethics of Cybersecurity* (Vol. 21).

Whitehead, G. (2020). *Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective*. *August*, 58.

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems*, *48*, 3–12. https://doi.org/10.1016/j.jmsy.2018.03.006

Zaqueu, P., & Mawela, T. (2023). *Factors Contributing to Cybersecurity Awareness , Education and Training*. *5*, 69–78.

Zitte, L.F. et al., 2012. (2012). No TitleФормирование парадигмальной теории региональной экономики. *Экономика Региона*, *12*(2), 115–121.

APPENDICES

Appendix I: Letter of Introduction

Sharon Ngunju

Strathmore Business School

Strathmore University

Email: sharon.ngunju@strathmore.edu

Dear Sir/Madam,

RE: DATA COLLECTION

I am a Master of Commerce student at Strathmore University Business School. I am conducting a study that involves collecting data for writing and compiling the final research dissertation. This is in partial fulfilment of the requirements of the Master of Commerce course.

I am carrying out research on '**Factors Influencing the Adoption of Cybersecurity in Large Manufacturing Companies in Nairobi County'**. The information obtained from your organization shall be treated confidentially and shall be used for academic purposes only. Your participation in facilitating this study is highly appreciated.

Kindly direct any queries to Sharon Ngunju through sharon.ngunju@strathmore.edu

Thank you in advance.

Yours faithfully,
Sharon Ngunju

Appendix II: Ethical Approval and NACOSTI Research License

Strathmore UNIVERSITY

9th May 2023

Ms Ngunju Sharon,
sharon.ngunju@strathmore.edu

Dear Ms Ngunju,

RE: Factors Influencing the Adoption of Cyber-Security in Manufacturing Companies in Kenya

This is to inform you that SU-ISERC has reviewed and **approved** your above **SU-masters** research proposal. Your application reference number is **SU-ISERC1720/23**. The approval period is from **9th May 2023 to 8th May 2024**.

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used.
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-ISERC.
iii. Death and life-threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-ISERC within 72 hours of notification.
iv. Any changes anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-ISERC within 72 hours.
v. Clearance for the export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to the expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days of completion of the study to SU-ISERC.

Before commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology, and Innovation (NACOSTI) https://research-portal.nacosti.go.ke/ and obtain other clearances needed.

Yours sincerely,

for: **Mr Ambrose Rachier,**
Chairperson; SU-ISERC

STRATHMORE UNIVERSITY INSTITUTIONAL SCIENTIFIC AND ETHICAL REVIEW COMMITTEE
(SU-ISERC)
09-May-2023
Email:ethicsreview@strathmore.edu
P.O BOX 59857-00200
NAIROBI-KENYA

REPUBLIC OF KENYA

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 765476

Date of Issue: 25/May/2023

RESEARCH LICENSE

This is to Certify that Ms.. Sharon Ngonjo of Strathmore University, has been licensed to conduct research as per the provision of the Science, Technology and Innovation Act, 2013 (Rev:2014) in Nairobi on the topic: FACTORS INFLUENCING THE ADOPTION OF CYBERSECURITY IN LARGE MANUFACTURING COMPANIES IN NAIROBI COUNTY for the period ending : 25/May/2024.

License No: NACOSTI/P/23/26137

765476

Applicant Identification Number

Director General
NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION

Verification QR Code

NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.

See overleaf for conditions

Appendix III: Research Questionnaire

This questionnaire aimed to collect information regarding the influence of adoption of cybersecurity in large manufacturing companies within Nairobi County.

Confidentiality clause

The responses you provide in this questionnaire will be used in strict confidence and solely for academic purposes advanced by this research.

SECTION A:

1. State your Gender

   Male [ ]

   Female [ ]

2. What is your age?

   Under 20 years [ ]

   21-30 years [ ]

   31-40 years [ ]

   41-50 years [ ]

   51 years and above [ ]

3. For how long have you been with the company?

   Less than 1 year [ ]

   Between 1 and 3 years [ ]

   Over 3 years [ ]

4. Level of education

   Certificate/Diploma [ ]

   Degree [ ]

   Masters [ ]

   PhD [ ]

5. Indicate the sector of your organization?

   ☐ Building, Mining and Construction

   ☐ Chemical & Allied

   ☐ Energy, Electricals & Electronics

   ☐ Food & Beverage

   ☐ Leather & Footwear

   ☐ Metal & Allied

   ☐ Automotive

   ☐ Paper & Paperboard

   ☐ Pharmaceutical & Medical Equipment

   ☐ Plastics & Rubber

   ☐ Service & Consultancy

   ☐ Textile & Apparels

   ☐ Timber, Wood & Furniture

   ☐ Agriculture/Fresh Produce

6. How many employees does your organization have?

   ☐ 100 – or less

   ☐ 101 – 999

   ☐ 1000 and above

7. What is the approximate annual business revenue turnover in Kenya Shillings?

   ☐ Less than 1 billion
   ☐ 1 – 10 billion
   ☐ 11 – 20 billion
   ☐ 21 – 50 billion
   ☐ Above 50 billion

8. What is your job role at the institution?

   ☐ Chief Information Officer (CIO)

   ☐ ICT Manager/Director

   ☐ Chief Information Security Officer

   ☐ ICT Officer/Systems Analyst/System

Administrator

9. How is cybersecurity managed at your institution?

☐ By vendors

☐ In house by IT expert

☐ In house computer emergency response team

☐ Outsourced to an independent specialized organization

SECTION B: FACTORS THAT INFLUENCE THE ADOPTION OF CYBERSECURITY IN LARGE MANUFACTURING COMPANIES IN NAIROBI COUNTY

Please indicate in the table with a tick (√) your level of agreement based on the below scale:

1= Strongly Disagree 2= Disagree 3= Neither Agree nor Disagree 4= Agree

5= Strongly Agree

No	Organizational resource factors	1	2	3	4	5
(1.)	The organization has adequate personnel with cybersecurity expertise.					
(2.)	The organization has adequate skills to implement and support new cybersecurity technologies.					
(3.)	The organization has internal cybersecurity staff. The organization does not rely on cybersecurity solution vendor support					
(4.)	Budget is a major constraint in the acquisition and implementation of new cybersecurity technologies for the organization.					
(5.)	High training costs of the cybersecurity team impede internal capacity development in the organization.					

(6.)	The organization has in house cybersecurity skills development programs to enhance staff cybersecurity skills.					
(7.)	The organization has set up ICT structures with HR strategies that determine the quality of new entrants into the organization.					

No	**Management Factors**	**1**	**2**	**3**	**4**	**5**
(1.)	The organization management ensures there is a cybersecurity awareness programs that staff are mandated to take part in.					
(2.)	The organization's management board has ICT competencies.					
(3.)	The leadership team in the organization positively influence employees' attitude towards cybersecurity awareness.					
(4.)	The top management ICT competency helps in determining the choice of technologies and tools that the organization adopts and how these are in turn updated over time.					
(5.)	The management has put in place adequate internal ICT/cybersecurity policies which they monitor regularly in the organization.					
(6.)	The organization management assesses the cost of potential cybersecurity breaches to determine the right level ofinvestment to mitigate the risk.					
(7.)	The organization's top management awareness about cyber attacks' success probability, influences higher investment in adoption of cybersecurity.					

(8.)	The organization's top management of your company is committed to ensuring a high level of cybersecurity.					

No	Technological factors	1	2	3	4	5
(1.)	The organization maintains confidentiality of privileged information stored in the organization's critical assets or ICT network.					
(2.)	The organization maintains integrity of information stored in the organization's critical assets or ICT networks.					
(3.)	The organization maintains availability of information stored in the organization's critical assets or ICT network.					
(4.)	The cost of cybersecurity incidences is not clear to the organization hence, affecting uptake of cyber insurance.					
(5.)	The organization has set a baseline configuration to guide the setup of infrastructure.					
(6.)	The organization cybersecurity technology has simplified steps for users to comprehend.					
(7.)	The organization cybersecurity technology is easy to operate in terms of ease of remembering and guidance.					
(8.)	The organization cybersecurity infrastructure is efficient, effective and improves performance and productivity.					

SECTION C: FACTORS THAT INFLUENCE THE ADOPTION OF CYBERSECURITY IN LARGE MANUFACTURING COMPANIES IN NAIROBI COUNTY

Please indicate in the table with a tick (√) your level of agreement based on the below scale:

1= Strongly Disagree 2= Disagree 3= Neither Agree nor Disagree 4= Agree

5= Strongly Agree

No.	Adoption of cybersecurity	1	2	3	4	5
	Threat and vulnerability assessment					
(1.)	The organization ensures all threats and vulnerabilities identified are mitigated and documented.					
(2.)	The organization classifies and prioritizes different cyber risks facing the institution on its critical assets.					
(3.)	The organization regularly performs cybersecurity assessment exercise.					
(4.)	The organization periodically does drill tests on the business continuity plan to check its adequacy.					
(5.)	The organization has access to threat intelligence reports directly related the organization.					
	Protection					
(6.)	The organization has valid user two-factor authentication (login and password).					
(7.)	The organization protection facility has antivirus and firewalls security features.					
(8.)	The organization has adopted services on Virtual Private Network or other remote access capability.					
(9.)	The organization has authentication and encryption for Wi-Fi access.					
(10.)	The organization limits access to logs, change logs and periodically reviews logging policies and procedures.					
	Detection					
(11.)	The organization detection facility has alerts for threats					
(12.)	The organization detection facility has the capability to check anomalies and report events.					

(13.)	The organization detection facility has inbuilt cybersecurity corrective processes.					
(14.)	The organization detection facility has an inbuilt cybersecurity audit logs reporting system.					
(15.)	The organization has threat intelligence teams that go through internal and external intelligence databases and remove any false positives.					
	Recovery (Response)					
(16.)	The organization response facility allows for efficient incidence turnaround time.					
(17.)	The organization has plans in place to ensure business operations continue in the event of an adverse scenario.					
(18.)	The cyber incident response plan for the enterprise is tailored to rapidly contain damages and mobilize response resources if a cyber incident were to occur.					
(19.)	The organization has documented plans for responding to and aid in recovering from cyber incidents that include recovery time objectives and recovery point.					
(20.)	The organization has a documented cybersecurity strategy.					

Thank you for participating in the research.

Appendix IV: Proposed Work Plan

FACULTY: SCHOOL OF BUSINESS

Title of Thesis: Factors Influencing the Adoption of Cybersecurity in Large Manufacturing Companies in Nairobi County

WORK PLAN

Progress Stage 1	Research Problem clarification, Research objectives, Purpose, and Significance	November-December 2022
Progress Stage 2	Literature Review	January-February 2023
Progress Stage 3	Proposed Research Methodology	January-February 2023
Progress Stage 4	Proposal Presentation	March 2023
Progress Stage 5	Data Collection	March-April 2023
Progress Stage 6	Data Analysis and Interpretation	April 2023
Progress Stage 7	Thesis report writing - first draft	May 2023
Progress Stage 8	A final draft of the research report	June 2023
Progress Stage 9	Submission of thesis for examination	September 2023
Progress Stage 10	Oral defense of the thesis	November 2023
Progress Stage 11	Correction of thesis	November 2023

Appendix V: List of Large Manufacturing Firms in Nairobi

Energy, Electricals and Electronics Sector	
East African Cables Ltd	Kenya Power & Lighting Co.
Eveready East Africa	Kenya Shell Ltd
Chemical Sector	
Procter & Gamble Eas	Sadolin Paints (E.A.) Ltd
Beiersdorf East Africa td	European Perfumes & Cosmetics Ltd
Unilever Kenya Ltd	Carbacid (CO2) Limited
Colgate Palmolive (E.A) Ltd	Chemicals and Solvents E.A. Ltd
Johnson Diversity East Africa	Excel Chemical Ltd
Vitafoam Products Limited	Galaxy Paints & Coating
Magadi Soda Company Ltd	Syngenta East Africa Ltd (1999) Ltd
PZ Cussons Ltd	Cooper Kenya Limited
BOC Kenya Limited	SupaBrite Ltd
E. Africa Heavy Chemicals	
Food Sector	
Aquamist Ltd	Wrigley Company (E.A.) Ltd
Premier Flour Mills Ltd	Softa Bottling Co. Ltd
Premier Food Industries Development Limited	Nestle Kenya Ltd
Proctor & Allan (E.A.) Ltd	Kenya Sweets Ltd
Candy Kenya Ltd	Kenya Nut Company Ltd
British American Tobacco	Kenya Breweries Ltd
Broadway Bakery Ltd	Karirana Estate Ltd
Coca Cola East Africa Ltd	Nairobi Flour Mills Ltd
Deepa Industries Ltd	NAS Airport Services Ltd
Highlands Mineral Water	Belfast Millers Ltd
Del Monte Kenya Ltd	Bidco Oil Refineries Ltd
Mount Kenya Bottlers Ltd	Kakuzi Ltd
East African Breweries Ltd	Kenya Wine Agency
East African Sea Food Ltd	London Distillers (K) Ltd
Manji Food Industries Ltd	Brookside Dairy Ltd
Kenya Tea Development Agency	Blowplast Ltd
Kevian	Kenpoly Manufacturers Ltd
Farmers Choice Ltd	Kingway Tyres & Automart Ltd
Kenafric Industries Limited	Packaging Industries Ltd
Kenblest Limited	Techpak Industries Ltd
Alpine Coolers Ltd	ACME Containers Ltd
Pembe Flour Mills Ltd	Haco Industries Kenya Ltd
Precision Plastics Limited	Sameer Africa Ltd
Safepak Limited	

Building Sector	
Kenbro Industries Ltd	Kenya Builders & Concrete
Paper Sector	
Chandaria Industries Limited	Kartasi Industries Ltd
Primex Printers Ltd	Kenafric Diaries
Dodhia Packaging Limited	Kitabu Industries Ltd
East Africa Packaging Industries Ltd	Pan African Paper Mills (EA) Limited
Jomo Kenyatta Foundation	Ramco Printing Works Ltd
Textile Sector	
Africa Apparels EPZ Ltd	Kenya Trading EPZ Ltd
Apex Appaels (EPZ) Ltd	ProtexKenya (EPZ) Ltd
Timber Sector	
Fine Wood Works Ltd	Twiga Stationers & Woodtex Printers Ltd
Hwan Sung Industries (K) Ltd	Shamco Industries Ltd
Furniture International Limited	Slumberland Kenya
Kenya Wood Ltd	Timsales Ltd
PG Bison Ltd	Tetra Pak Ltd
Motor Vehicle Assembly and Accessories Sector	
Bhachu Industries Ltd	Mann Manufacturing Co. Ltd
General Motor East Africa	Isuzu Ltd
Associated Battery Manufacturers Ltd	
Metal and Allied Sector	
Allied Metal Services Ltd	Orbit Engineering Ltd
Heavy Engineering Ltd	Sheffield Steel Systems Ltd
Metal Crown Limited	Davis & Shirtliff Ltd
Tononoka Steel Ltd	
Pharmaceutical and Medical Equipment Sector	
Beta Healthcare International Limited	KAM Pharmacy Limited
GlaxoSmithkline Kenya Ltd	Pharm Access Africa Ltd
Leather Products and Footwear Sector	
Bata Shoe Co. (K) Ltd	Leather Industries of Kenya Limited
C & P Shoe Industries Ltd	