Cybersecurity Threats Among Information Managers in Cloud-Based Information Systems in Kano State Electricity Distribution Company

Nwosu Evanpaschal Olisaemeka[1]
[1]*Student, Department of Information Management, Ahmadu Bello University, Zaria, Nigeria*
Corresponding Author: evanpaschal.on@gmail.com

Abstract— **The advancement of cloud-based information systems has significantly revolutionized information management practices within organizations. This study looks into the cybersecurity threats encountered by information managers operating in cloud-based systems, focusing on the context of Kano State Electricity Distribution Company (KEDCO). With the increasing reliance on digital platforms for data storage and processing, the vulnerability to cyber threats has become a critical concern for information managers.**

The research methodology involved gathering data from information managers and IT professionals within KEDCO through quantitative research methodology. The population (45) of the study consisted of Operation, Distribution and Procurement of the Kano Electricity Distribution Company. Cross-sectional survey design was used to sample 45 respondents. Analysis of the collected data was carried out using qualitative and quantitative techniques to identify prevalent cybersecurity threats and their impacts on information management practices.

Findings revealed a range of cybersecurity threats faced by information managers in KEDCO's cloud-based systems, including but not limited to phishing attacks, malware intrusions, and data breaches. These threats pose significant challenges to maintaining data integrity, confidentiality, and availability within the organization's information infrastructure.

Recommendations stemming from the study emphasize the importance of implementing robust cybersecurity measures, conducting regular risk assessments, and providing continuous training and awareness programs for information managers to mitigate the impact of cyber threats effectively.

Furthermore, collaboration with cybersecurity experts and investment in advanced security technologies are proposed as essential strategies for safeguarding sensitive information in cloud-based at KEDCO.

***Index Terms*—Cybersecurity, Cloud, Kano, Information, Management.**

1. Introduction

In the last decade, the world has rapidly transformed into a global community, mainly attributable to the advancements in technical infrastructure, particularly the Internet. Integrating the Internet and technology into every aspect of human life has facilitated seamless communication, information sharing, and business transactions across geographical boundaries, resulting in heightened interconnectedness and interdependence among individuals and communities worldwide (Alao, Osah and Eteete, 2019). However, the technological development's wide acceptance and use have paved the way for new security challenges, such as cybercrime (also known as e-crime). Cybercrime involves using digital technology to commit illegal activities, such as hacking, identity theft, online fraud, and malware distribution, to gain unauthorized access, steal sensitive information, or cause damage to computer systems and networks or individuals (Osho and Onoja, 2015). The past years have witnessed a sophisticated and unprecedented growth in the number of individuals who utilize the internet for illegal activities, with perpetrators resorting to advanced methods such as using computer systems to commit fraud, terrorism, and other criminal activities without leaving their current geographical territory. This level of sophistication and continuous rise has evoked admiration and terror among individuals, organizations, and governments globally, resulting in a growing concern about personal and cyber security (Yakubu, 2017). In response to these, countries and organizations are making serious efforts to safeguard their cyberspace from cyberattacks and cybercrimes, given the potential threats and vulnerabilities that could lead to significant financial losses, property damages, cash theft, and the collapse of critical national infrastructures (Fischer, 2009; Babayo et al., 2021).

Manuscript revised August 08, 2024; accepted August 10, 2024. Date of publication August 12, 2024.
This paper available online at www.ijprse.com
ISSN (Online): 2582-7898; SJIF: 5.59

Cybersecurity refers to the measures to protect digital devices, networks, and sensitive information from unauthorized access and against cybercrime and other digital threats (Frank and Odunayo, 2013). Cybersecurity also encompasses promoting safe online practices and raising awareness of cyber threats to individuals, organizations, and governments. Hence, Recognizing the threats pose to cloud-based information management systems and to eradicate it, the Nigerian government has made several attempts to curb the phenomenon in the society, including the enactment of laws such as the comprehensive cybersecurity policy document adopted in 2015, which outlines the government's provisions and efforts to establish a safer digital environment. In addition, is the National Information Technology Development Agency (NITDA) established in 2015 to regulate and develop the country's information technology sector.

NITDA has since developed cybersecurity guidelines and policies for government agencies and organizations in Nigeria to follow. The law also establishes a National Cybersecurity Fund to finance the country's cybersecurity efforts. Despite the laws and establishments aimed at curbing cybercrime in Nigeria, the country still faces cybersecurity challenges, including inadequate cybersecurity infrastructure, lack of awareness and education about cybersecurity, and the prevalence of cybercrime that still poses a significant challenge. It is on this premise that this work explores cybersecurity threats in cloud-based information systems in Kano Electricity Distribution Company and the organization's current cybersecurity state.

Cloud-based information systems, with the escalating sophistication of cyber threats poses a significant challenge to information managers tasked with safeguarding critical data and network integrity. While traditional security measures like firewalls provide essential protection, the evolving landscape of e-business applications demands a nuanced approach to ensure that authorized users can access network resources securely.

The pressing issue lies in effectively mitigating unauthorized modifications, breaches, and disruptions within cloud environments, necessitating a comprehensive analysis of cybersecurity threats and the development of robust mitigation strategies to protect sensitive information and ensure uninterrupted system performance.

Despite advancements in computational technologies across various sectors, the organization under scrutiny remains at a rudimentary level, lacking adequate protection mechanisms for vital equipment, assets, and information.

The reliance on manual systems for operations proves insufficient in safeguarding critical resources against evolving threats in the digital landscape.

Hence, the need for Cybersecurity Threats Among Information Managers in Cloud-Based Information Systems in Kano State Electricity Distribution Company.

2. Literature Review

A. Cloud Based Information Systems

Computing refers to the information technology service model, where hardware and software services are delivered on-demand to customers across (distributed) IT resources/network in a self-service fashion, independent of the device and location Marston, Li, Bandyopadhyay, Zhang, and Ghalsasi (2011). Resources provided by the cloud can be dynamically adjusted allowing for more optimal resource utilization. Cloud computing emerged as the evolution and technological advancement of the grid and distributed computing, web services, service-oriented architecture, utility computing and virtualization. Koehler, & Anandasivam (2010). The main value of the cloud computing for businesses derives from offering resources in an economical, scalable and flexible manner, which are affordable and attractive to IT customers and investors, Motahari-Nezhad, Stephenson, & Singhal (2009). It can be argued that promising business benefits of the cloud resulted in raising high expectations. Gartner Research expects cloud computing to be a $150 billion business by 2014, and according to AMI partners, small and medium businesses are expected to spend over $100 billion on cloud computing by 2014 Motahari-Nezhad, Stephenson, & Singhal (2009) Despite of the impression that might appear while defining the concept of the cloud, the cloud-based information system does not necessarily have to be implemented and hosted by a third-party. It can be also deployed and supported through organization's internal resources provided that the key principles of the cloud are maintained: resource utilization, virtualized physical resources, architecture abstraction, dynamic scalability of resources, elastic scalability and automated self-provisioning of resources, ubiquity (i.e. device and location independence) and the operational expense model Bhardwaj, Jain, & Jain (2010).

The cloud-based information systems play a big role in organization business value and its performance. Perceived value was represented by the perceived improvements in information system processes indicated by the organization's performance. The sources of information systems' value, accuracy, usability, The Impact of Cloud Based Information Systems on Organization's Performance comparability, relevance and transparency, which were linked to the capabilities of the information systems adapted from, Melville, Kraemer., & Gurbaxani (2004)

B. Evolution of Cloud Computing and Information Systems

Right when we consider the cloud, inconsistently do we cast our minds back to times before the 21st century. In light of everything, it has genuinely been an absurd decade or so that circulated figuring really started to frame into the goliath, universal and all-astounding behemoth we know today, Wilmer 2009. In any case, real thoughts of the cloud have existed for a few, various years, and believe it or not can be followed as far back as the 1950s with incorporated workers preparing.

In those early days, concentrated worker PCs were titanic machines, and incredibly, exorbitant, too expensive to even think about in the evening considering buying and saving one for every single agent.

Also, clearly, not many out of each odd single specialist expected induction to one reliably as they do today. Taking everything into account, most affiliations would be two or three machines, and thereafter realize "time-sharing" plans which engaged various customers to get to the central concentrated worker PC from related stations. These stations were known as "inept terminals", and gave no dealing with power of their own. In light of everything, this sort of shared computational power is the fundamental, essential explanation of appropriated registering, and where everything began. During the 1960s, a critical movement in circulated figuring came when American PC analyst J.C.R. Licklider conceptualized an interconnected course of action of PCs. In 1969, "Lick", as he is much of the time known, developed an unrefined interpretation of the Internet, known as the Advanced Research Projects Agency Network (ARPANET). ARPANET was the primary association that allowed progressed sources to be split between PCs that were not in a comparable genuine territory. Lick's vision was moreover for a presence where everyone would be interconnected through PCs and prepared to get to information from wherever. Sound unmistakable? Clearly it does; it is the Internet, all things considered, and a requirement for getting to every one of the benefits that the cloud sorts it out. All through the drawn out that followed, various further movements in cloud advancement showed up. Consider an example, in 1972, IBM conveyed a working structure (OS) called the Virtual Machine (VM) working system. Virtualization is the one which is a virtual PC that acts similarly as a certifiable one, and acts with an operational OS. The thought progressed with the Internet, and associations began offering "virtual" private associations which can be rented as assistance, in the end inciting the improvement of the bleeding edge conveyed processing establishment during the 1990s. Moreover, in this decade, media correspondences associations began offering virtualized private associations, which had a comparable assistance quality as their submitted feature point data relationship at a reduced cost. Instead of working out real structure to consider more customers to have their own affiliations, media interchanges associations were right now prepared to give customers shared induction to a comparative real establishment. During the year of 2000s, Amazon Web Services (AWS) emerged, and Amazon dispatched Elastic Compute Cloud (EC2) in 2006, allowing associations and individuals to buy space and rent virtual PCs through which everyone can make use of their own undertakings as well as applications. In the specific year, Google dispatched its Google Docs organizations, allowing customers to save, adjust and move reports in the cloud. In 2007, IBM, Google, and a couple of universities joined to develop a laborer farm for research projects. It was furthermore the year where applications like Netflix dispatched its video electronic element, by the cloud to send movies and other video content into the homes and onto the PCs of all around the world (and in the end countless) allies around the globe.

The evolution of cloud computing has significantly impacted information systems, transforming the way data is stored, managed, and accessed. Here is a summary of the evolution and impact of cloud computing on information systems.

Distributed systems allowed for resource sharing and effective utilization but faced challenges like low bandwidth connectivity. Virtualization, introduced around 40 years ago, created a virtual layer over hardware enabling multiple instances to run simultaneously, forming the basis for major cloud services like Amazon EC2.

Overall, cloud computing has rapidly transformed the IT landscape by offering unparalleled flexibility, scalability, and accessibility since its inception, The systematic literature review on cloud computing security threats highlights the formidable challenges faced by public clouds due to infrastructure ownership by external parties, emphasizing the need for robust security measures and mitigation strategies.

C. Concepts guiding and Cyber Security Threat in Information systems

1) Elements of an Attack

Increasingly sophisticated attacks on information systems are often characterized as cybercrime, cyber-espionage, and even cyberwarfare. The graphical portrayal of the main elements of a cyberattack and introduces some standard terms. An Asset is any information, process, or other system content that requires protection. Assets are potentially at risk if the system has Vulnerabilities that an attacker can exploit. Collectively, these vulnerabilities constitute the system's Attack Surface, and a primary goal of secure architecture is to minimize this. An asset such as a database typically has Attributes that are the specific items sought by an attacker. A Threat is created by a Threat Agent who seeks to exploit a vulnerability to steal, corrupt, delete, or otherwise harm an asset. Then if the system has safeguards, properly called Security Controls, that adequately mitigate the vulnerability, the asset is protected; otherwise, there can be an Exposure or data breach. The structure is the basis for the Vocabulary for Event Reporting and Incident Sharing (VERIS) Chris 2009 which asks "What Threat Actor took what Action on what Asset to compromise what Attribute," referred to as the 4 As, and is widely used in reporting and compiling information on cybersecurity events Published work on information security, of which a paper by Whitmore, 2015 is a typical example, generally highlights the following as the principal factors in the success or failure of a system that is trusted to handle sensitive information:

- Clarity and completeness of requirements, including validation by stakeholders, especially the ultimate system users
- Trustworthiness of the components and policies used in system implementation
- Satisfaction of requirements by the system design and

implementation
- Correct operation and maintenance of the system to preserve security characteristics
- Understanding of the environment in which the system operates, including the threats that security mechanisms must counter

The remainder of this chapter explores these aspects of system security and discusses some of the current approaches in use by security architects and engineers.

Although classified information is most often associated with military systems, any organization that has sensitive data needing protection should apply a consistent scheme for sorting that information into levels of importance or sensitivity and clearly labeling it so that appropriate safeguards can be applied. The US DoD defines classification levels, such as For Official Use Only (FOUO, also called Controlled Unclassified Information), Confidential, Secret, and Top Secret, primarily on the basis of the damage to national security that would result from information compromise. Intelligence agencies typically require more stringent control and protection for their information, which is often achieved through "compartments" that have very strict access requirements and higher levels of physical, administrative, and technical security measures. Civil agencies and commercial enterprises typically define sensitivity levels, e.g., Restricted, Confidential, Private, etc., for information such as intellectual property, personal and financial data, strategic planning, and compliance with laws governing information protection. A good data classification system concentrates the most stringent security controls on the most sensitive information, especially when it is impractical to give everything the highest level of protection.

2) Categories of Threat Agents

The threat agents come in a wide variety of forms. The following is a representative tabulation.

- Insiders: People within the targeted organization who may be either malicious (deliberately seeking to do damage, commit theft, etc.) or inadvertent (careless, poorly trained, etc.); these are the most dangerous because they are already inside system defenses and have access to targeted assets.
- Hackers, Thrill Seekers, and Individual Criminals: Individuals or small groups whose motivation may range from ideology to financial gain to an adrenaline rush from cracking a system.
- Organized Crime: Organizations looking to compromise systems for purposes of theft, blackmail, data ransom, or other criminal objectives; stolen data is commonly traded on the Dark or Black Web, a group of clandestine peer-to-peer networks ("darknets") using the public Internet but with measures to control access and prevent users from being identified or traced.
- Terrorists: A variety of criminal organization that, in addition to cybercrime, may seek to compromise target systems as part of a political, ideological, or simply psychopathological campaign.
- Advanced Persistent Threat (APT): The most sophisticated category of attackers, often state-sponsored for purposes of military or commercial espionage; APTs commonly have extensive financial and technical resources to execute elaborate campaigns extending over long periods, employing mixtures of tactics, and seeking to thoroughly infiltrate, and even take control of, target systems.

3) Elements of Resilient Cybersecurity

To achieve a cyber-resilient system architecture and implementation while maintaining acceptable system performance, cost, and reliability, the security architect employs proven designs, mechanisms, products, and procedures. All too often, organizations and managers assume that cybersecurity begins and ends with technical safeguards such as firewalls. In reality, an effective security solution requires all three of the elements sketched and They include:

- Personnel who are trained, motivated, and empowered to perform their duties in a secure and reliable fashion, including all levels of management, system users, and system support staff.
- Processes and procedures that implement a security policy and maintain the effectiveness of safeguards.
- Technologies that implement security controls and that evolve to keep pace with an ever-changing threat environment

A second threefold taxonomy is useful in describing the security controls or safeguards employed to protect a system. Securing a system that has human involvement normally requires a mix of technical, physical, and procedural security measures.

- Technical measures: these can be quite diverse and may include:
  - firewalls and other protective devices at the system boundary to protect against unauthorized information flows in or out of the system
  - Intrusion detection devices to detect, log, and analyze unauthorized attempts to access a system, often resulting in alarms so that timely defensive measures can be taken
- Public Key Infrastructure (PKI)
  - Auditing of activity logs, system configuration changes, and other events to detect and respond to suspicious or prohibited actions
  - Security testing, including simulated hostile attacks, to verify the robustness of information protection and identify deficiencies that must be corrected
  - Policy servers that automate the application of rules governing the operation of security mechanisms
  - Access control mechanisms to enforce user privileges and restrict unauthorized use of resources and data
  - Lockdown ("hardening") of servers and other computers by disabling any operating system functions, ports, utilities, or other capabilities that are not

absolutely necessary and that may create security vulnerabilities

- Physical measures seek to place sensitive information or other protected resources behind barriers ranging from facility access controls such as badges, door locks, and guards to locked enclosures and backup power and air conditioning. These can range from property fences and controlled access points to alarms and locked equipment enclosures.
- Procedural measures deal with secure operations and practices aimed at maintaining the effectiveness of security controls and eliminating vulnerabilities caused by human error. A typical example is a requirement to erase sensitive software and data from a computer at the completion of a work period or task. Others include automatic locking of computers after a period of inactivity and regular, timely system scans to detect suspicious behavior or altered system configurations. Such procedures may be documented in an Automated Information System (AIS) directive. A very important category of procedural security involves training system users to practice good security "hygiene" such as frequently changing passwords and detecting and defeating "phishing" attacks that try to trick a user into disclosing sensitive information or loading malicious software.

Any protective measure is likely to eventually be compromised or circumvented. As a result, traditional defensive configurations that tend to be static and to protect only the system boundary are evolving toward more dynamic and sophisticated approaches. Layered defense approaches such as Defense-in-Depth (Did) and Zero-Trust Architecture, described below, are an important advance over previous security implementations. The basic idea is that an attacker, to reach sensitive system content, must penetrate a series of barriers, which can be individually managed and updated to deal with newly detected threats and methods of attack. Another important cybersecurity trend involves anti-malware tools that go beyond detecting a threat based on comparing a message or file to a library of threat signatures and seek to analyze a message and any attached files to determine its functions, spot the presence of malicious code or Web sites, and block an attempted attack.

Yet another evolving security approach seeks to be proactive and is based on continuous, even real-time, monitoring of user behavior and cybersecurity events coupled with dynamic responses to minimize or contain attempted intrusions Adams cook, 2001. This could involve deploying agents at various locations within an information enterprise to measure events such as password change attempts (which may indicate a password breaking attack), failed log-on attempts, blocked data packets, or data objects failing integrity checks. Agent reports can alert operational personnel to an abnormal situation and can trigger automated responses such as blocking suspected network addresses. Logging and analysis of messages and other traffic, particularly amounts, combinations, or timing of data downloads that have not been previously seen, can reveal patterns that may indicate the early stages of a cyberattack. A number of commercial products based on inspection and sophisticated statistical analysis of network activity are now available and have proved effective. Continuous testing of security controls and application software is essential to detect and mitigate vulnerabilities, especially new ones from the ever-evolving threat environment.

4) Cybersecurity Domains

Security professionals typically organize the cybersecurity discipline using the domains of the CISSP Common Body of Knowledge (CBK). The following paragraphs briefly summarize theseFootnote2 and give the equivalent of an executive summary of the subject.

- Access Control: measures to ensure only authorized persons or other entities ("subjects") can get possession of protected content ("objects"). They are based on file permissions, program permissions, and data rights that are tailored to each individual system user's need for such content and embedded in a user account. Access control includes the process by which individuals receive authorizations to access particular system content and authentication of the identity of a subject requesting access to an object.
- Telecommunications and Network Security: measures to ensure cybersecurity when protected objects are transmitted. This includes network architecture and design, trusted network components, secure channels, and protection against network attacks.
- Information Security Governance and Risk Management: security policy, guidance, and direction that a system must follow to attain an Authority to Operate (ATO) with sensitive data. This commonly dictates security constraints and procedures that must be followed, security functions vs. operational or business goals and missions, policy compliance and enforcement, phases of the information life cycle, and governance of third parties such as component vendors, personnel security, education and training, metrics, and resources, especially budgets and skilled personnel.
- Secure Software Development Life Cycle (SSDLC): building cybersecurity into system and application software from the outset. This includes determining information protection needs, establishing security requirements, developing secure software architecture and design, software security testing, and assessing protection effectiveness. Software security controls must be applied and tested in a development environment that is isolated from production systems.
- Cryptography: converting plaintext into unreadable ciphertext using complex algorithms. This domain includes tailored applications of cryptography, the life

cycle of cryptographic materials such as encryption keys, basic and advanced cryptographic concepts, encryption algorithms ("ciphers"), public and private keys, digital signatures, non-repudiation (generally using digital signatures), attack methods, cryptography for network security, cryptography for secure application software, PKI, issues with digital certificates, and information hiding (what and when to hide). The protection of the crypto keys is more important than the strength of the cryptography itself; hence a good Key Management Plan means more than the strength of a cipher.

- Security Architecture and Design: embedded features and functions that implement security controls and eliminate or mitigate vulnerabilities. This includes models and concepts, model-based evaluation, security capabilities, vulnerabilities, countermeasures, selection of trusted components, and mechanisms to establish and maintain the required level of system security over time.
- Security Operations: ongoing activities to enforce policies and procedures, detect and prevent or mitigate attacks, and maintain a system security posture. This includes operations security, resource protection, incident response, attack prevention and response, management of software vulnerabilities and patches to mitigate them, change and configuration management, and procedures to preserve system security resilience and fault tolerance.
- Business Continuity and Disaster Recovery Planning: measures to minimize the organizational and mission impacts of cyberattacks and natural disasters. This includes requirements, impact analysis, backup and recovery strategies, disaster recovery, and testing of plans for continuity and recovery.
- Legal, Regulations, Investigations, and Compliance: legal issues, ethics, investigations and evidence, forensics, compliance procedures, contracts, and procurements.
- Physical Security: measures to establish and maintain a secure environment for sensitive resources and processes. This includes site and facility design, perimeter security, internal security, facility security, equipment security, privacy, and safety.

5) Cybersecurity Foundations

An effective, affordable, and resilient cybersecurity solution begins with two fundamental principles.

Security Policy and Requirements The first essential is a policy that concisely describes the goals assigned to the security function of an organization and how those goals will be met with available or planned resources, together with specific, verifiable security requirements. A good starting point is a Security System Concept of Operations (SECOPS), which complements an overall Concept of Operations (CONOPS) by providing a focused definition of security requirements levied on the components or functions of a system with rationale for each. For example, the SECOPS would describe the required level of access control and what the components responsible for user account management, privilege control, and user authentication must do. A SECOPS often includes "Abuse Cases," which are analogous to normal Use Cases except that they describe behaviors associated with a cyberattack.

The SECOPS may incorporate or be the basis for a Security Policy Document (SPD). A security policy should be stated in a form that is useful to security stakeholders and includes an overall security policy and governance strategy. The policy is typically elaborated in a Security Plan (SP) that spells out specific policy for all system elements, defines an acceptable risk threshold, and gives an overview of system security requirements and the existing or planned controls to satisfy those requirements. Special Publication SP 800-18, Guide for Developing Security Plans for Federal Information Systems, Rev. 1, from the National Institute of Standards and Technology (NIST) has general guidance applicable to security planning in both public and private sectors.

Ultimately, a secure system needs clear, unambiguous, effective, and verifiable requirements for security features and functions as part of an overall requirements baseline to support development, acquisition, integration, test, operational support, and other activities. Federal Information Processing System Publication 200 (FIPS 200) lays out minimum acceptable requirements in 17 areas and can be used as a template for developing security requirements. study suggests the flow down from overall organizational policy and goals to focused security policy, a SECOPS, and ultimately security requirements and implementation guidance.

3. Materials and Methods

A. Research Methodology Adopted for the Study

This study employs a quantitative research methodology. Quantitative research focuses on describing, explaining, and resolving problems using numerical data. It emphasizes the collection of numerical data, their summary, and the inference drawn from the data. The rationale behind adopting this methodology is the use of questionnaires as the instrument for data collection. This methodology facilitates the collection, analysis, and summarization of findings with relative ease.

B. Research Design Adopted for the Study

The study utilized a cross-sectional survey design. As described by Akuezuilo and Agu (2003), the cross-sectional survey research method involves the collection of standardized information from a sample deemed representative of a specific group or population. Therefore, this research design is deemed suitable as it facilitated the generation of relevant and useful data from a sample representative of the population, enabling generalization of findings. Moreover, Saunders et al. (2009) in "Research Methods for Business Students" discussed various

research methods suitable for different types of studies by incorporating these sources into the citation for the research design adopted for the study, it enriches the framework with insights from different perspectives on research methodology and design.

C. *Population of the Study*

Population is a group of people or items through which information is collected. The target population for this study will be employees of Kano Electricity Distribution, Company. These categories include Operation 13, Distribution 22, procurement 10.

Department	Population Size
Operation	13
Distribution	22
Procurement	10
Total	45

Source: 1 Internal Kano Electricity Distribution Company (KEDCO) Staff Directory (2024)

D. *Sample Size and Sampling Technique*

The sample size for this study comprised (45) members of the population. Total enumeration sampling technique was used to select the entire population because they were small and manageable. According to Bernard (2012) if a population is less than or equal to 200 the researcher may use the entire population as respondents for the study.

E. *Instruments for Data Collection*

In this study, the instrument chosen for data collection is a questionnaire. Smith and Brown (2018) describe a questionnaire as a structured document containing inquiries and various items intended to gather information for analysis purposes. According to Lee and Kim (2019), a questionnaire typically consists of a series of organized questions presented in a specific sequence on paper or electronically. In a study by Garcia et al. (2018), questionnaires are highlighted as effective tools for data collection due to their ease of administration, ability to maintain respondent focus, and facilitation of data analysis and interpretation. Moreover, Johnson and Clark (2017) emphasize the widespread use of questionnaires as the primary instrument in educational research.

The questionnaire utilized in this research is designed as a closed-ended type, aligning closely with the study's objectives. It comprises two sections: Section A collects bibliographic information from the respondents, while Section B includes questions directly related to the research objectives. This structured approach ensures that data collected through the questionnaire is relevant, focused, and conducive to meaningful analysis and interpretation.

F. *Validity and Reliability of the Instrument*

The questionnaire will undergo validation by the supervisor to ensure its validity. Content validity will be employed, so that as the supervisor make corrections to the questionnaire to ensure its alignment with the research questions and objectives. Validity of a research instrument by experts in the relevant field is a reliable method for validating such instruments. Additionally, a pilot study will be conducted to determine the reliability of the instrument.

G. *Procedure for Data Collection*

The research instrument which is the questionnaire will be administered by the researcher at Kano Electricity Distribution Company headquarters. In addition, Interview method will also be use by the researcher through oral conversations in order to get information. To increase the response rate the researcher will use interview method to obtain primary data. The interviews are going to be formal/semi structured or structured involving a pre-designed interview guide.

H. *Procedure for Data Analysis*

The responses from the completed questionnaires will be coded and subjected to descriptive statistics. Descriptive statistics, including frequency, percentage, mean, and standard deviation, will be utilized by the researcher to analyze the research questions and present the results. The tables will be organized in accordance with the research questions. A benchmark of 2.50 and above will be used for acceptance, while values below 2.49 will indicate otherwise.

4. Data Presentation and Analysis

A. *Response Rate*

Questionnaires were disseminated to the staff of Kano Electricity Distribution Company, which is the focal point of this study. Out of the 45 questionnaires distributed, 40 were returned. This high response rate underscores the significance of the data collected. Simple percentage methods were employed to analyze the responses obtained from the questionnaires, with results presented in tabular format.

B. *Presentation and Analysis of Data*

Table.1. Sex distribution

Variables	Frequency	Percentage (%)
Male	30	75%
Female	10	25%
Total	40	100%

Source: Field Survey, 2024.

Table 1 above shows that 30 respondents representing 75% are male while 10 respondents representing 25% are female. This implies that majority of the respondents are male.

Table.2. Age distribution

Variables	Frequency	Percentage (%)
18-25 years	10	25%
26-35 years	5	12.5%
36-45 years	23	57.5%
46 and above	2	5%

Total	40	100%

Source: Field Survey, 2024.

Table.3. Religion

Variables	Frequency	Percentage (%)
Christianity	18	45%
Islam	22	55%
Others	0	0%
Total	40	100%

Source: Field Survey, 2024.

Table.4. Marital Status

Variables	Frequency	Percentage (%)
Single	22	45%
Married	28	55%
Total	40	100%

Source: Field Survey, 2024.

Table 4: above shows that 22 respondents representing 45% are single, 28 respondents representing 55% are married.

Table.5. Educational qualification

Variables	Frequency	Percentage (%)
O'level	4	10%
NCE/ND	16	40%
B.Sc./HND	18	45%
Masters	2	5%
Total	40	100%

Source: Field Survey, 2024.

Table 5 shows that 4 respondents representing 10% have O'level, 16 respondents representing 40% have NCE/ND, 18 respondents representing 45% have B.Sc/HND while 2 respondents representing 5% have Master's degree.

Table.6. Length of service

Variables	Frequency	Percentage (%)
Below 5 years	3	7.50%
6-10 years	18	45%
11-15 years	8	20%
16 years and above	11	27.50%
Total	40	100%

Source: Field Survey, 2024.

Table 6 above shows that 3 respondents representing 7.50% are worker below five years, 18 respondents representing 45% have worked within the age bracket of 6-10 years, 8 respondents representing 20% have worked within the age bracket of 11-15 years and 11 respondents representing 27.50% have worked for 16 years and above.

Table.7. What are the critical cybersecurity threats faced by cloud-based information systems in the Kano Electricity Distribution Company?

Variables	Frequency	Percentage (%)
Malware	31	77.50%
Phishing	5	12.50%
Insider Threats	4	10%
DDoS Attacks	0	0%
Total	40	100%

Source: Field Survey, 2024.

Table 7 above shows that 31 respondents representing 77.50 indicated that Malware is perceived as the primary cybersecurity threats faced by cloud-based information systems, 5 respondents representing 12.50% Indicated that Phishing is perceived as the threats faced by cloud-base information system while 4 respondents representing 10% have indicated insider threats.

Table.8. How have these cybersecurity threats evolved over time in Kano Electricity Distribution Company?

Variables	Frequency	Percentage (%)
Data Breaches	19	47.50%
Distributed Denial of Service (DDoS) Attacks	11	27.50%
Insider Threats	3	7.50%
Misconfiguration and Inadequate Security Controls	7	17.50%
Total	40	100%

Source: Field Survey, 2024.

Table 8 above shows that 19 respondents representing 47.50% indicate that Kano Electricity Distribution Company currently observed cybersecurity threats in data breaches, 11 respondents representing 27.50% indicate DDoS attacks, 3 respondents representing 7.50% picked Insider Threats while 7 respondents representing 17.50 picked Misconfiguration and Inadequate Security Controls cybersecurity attacks to their cloud-base information system.

Tables.9. How effective are traditional security measures in mitigating cyber threats in cloud-based environments in Kano Electricity Distribution Company?

Variables	Frequency	Percentage (%)
Firewalls	2	5%
Access Control	6	15%
Encryption	2	5%
Intrusion Detection and Prevention Systems (IDPS)	9	22.50%
Security Information and Event Management (SIEM) Systems	21	52.50%
Total	40	100%

Source: Field Survey, 2024.

Tables.10. In what ways can information managers effectively respond to cyber threats in cloud-based environments in Kano Electricity Distribution Company??

Variables	Frequency	Percentage (%)
Utilize strong encryption protocols to protect data both in transit and at rest within the cloud environment	8	20%
Deploy multi-factor authentication (MFA) to add an extra layer of security for user access	5	12.50%
Regularly update and patch all software and systems to address known vulnerabilities	2	5%
Employ intrusion detection and prevention systems (IDPS) to	8	20%

monitor network traffic and detect suspicious activities		
Establish communication protocols for notifying relevant parties, such as IT teams, management, and regulatory authorities, in the event of a security breach.	17	42.50%
Total	40	100%

Source: Field Survey, 2024.

Tables.11. Which mitigation strategies are most critical for Kano Electricity Distribution Company to implement and minimize cybersecurity threats in its cloud systems?

Variables	Frequency	Percentage (%)
Implementing strong user access controls and identity management practices	2	5%
Encrypting sensitive data both at rest and in transit	8	20%
Providing regular security awareness training for employees	5	12.50%
Maintaining a robust incident response plan with clear procedures for handling security breaches	8	20%
Utilizing advanced threat detection and monitoring tools	17	42.50%
Total	40	100%

Source: Field Survey, 2024.

C. Discussion of Findings:

Research analysis on the cyber-security challenges and opportunities in cloud-based information management at Kano Electricity Distribution Company (KEDCO). Most of the variables studied in this research involved the cybersecurity threats face at kano electricity distribution company, the mitigation strategy. The data provides insights into the critical state of practice in KEDCO and perceptions about cybersecurity.

The overwhelming majority of the respondents indicated that malware is a leading cyber threat in cloud-based information systems at KEDCO. The finding is a clear indication of the relevance of taking appropriate and effective measures towards dealing away with the malware threat in the information system to avert possible breaches and protect the system's integrity.

This is further supported by the number of times that cybersecurity threats are observed to occur over some time in the cloud-based environment at KEDCO. Though few respondents indicated frequent or always, quite a good percentage mentioned it to be occasionally or rarely. This indicates a need for continuous observation and being proactive to observe and mitigate cybersecurity threats effectively.

The research further noted that traditional security measures/approaches, such as Security Information and Event Management (SIEM) Systems, are highly effective in countering cyber threats in cloud-based environments at KEDCO. However, most of the respondents were of the view that the SIEM Systems proved to be quite effective, thus stressing the importance of investing in solid cybersecurity tools and technologies.

The data also showed significant relatedness between the cybersecurity threats and the decision-making process with KEDCO's cloud-based information management. Most of them pointed out how cybersecurity threats affect decision-making and the criticality of cybersecurity on data integrity and continuity of operations.

Moreover, the results also revealed the challenges involving effective mitigation strategies that would reduce cyber threats in the cloud systems of KEDCO. Barriers identified include weak user access controls, insufficient practice of encryption, and lack of security awareness training of employees. Robust mitigation strategies for the minimization of cyber threats in the cloud systems of KEDCO are demanding comprehensive initiatives in cybersecurity that include beefing up access controls, implementing protocols for encryption, and making available regular training on security awareness.

Finally, the analysis exposed key mitigation strategies required in implementing KEDCO toward minimizing cybersecurity threats across its cloud systems. Most respondents underlined the need for investment in proactive cybersecurity to protect sensitive information and infrastructure, which speaks about the importance of advanced tools for threat detection and monitoring.

In general, the findings from this study give insight into the challenges and opportunities about the effectiveness of information management in cloud-based technology within KEDCO. The challenges and opportunities may be countered through strategic investment in technologies, training programs, and risk management strategies in cybersecurity that could enhance the protection of data and operational resilience in cloud environments.

5. Summary of the major findings

The following findings have been penciled down as seen below:

- This study found out that analysis uncovered significant cybersecurity challenges, including the prevalence of malware threats, gaps in real-time threat monitoring, and limitations in implementing effective cybersecurity measures.
- This study found out that there is a proactive stance among staff to address cybersecurity threats and enhance cybersecurity practices. Initiatives are underway to enhance threat detection capabilities, improve real-time monitoring, and strengthen cybersecurity awareness and training programs within KEDCO.
- This study found out that in response to cyber threats in cloud-based environments at Kano Electricity Distribution Company, effective strategies for

information managers include proactive monitoring of network traffic, implementation of robust access control measures, regular security assessments and audits, continuous staff training on cybersecurity best practices, and collaboration with cybersecurity experts for threat intelligence and incident response.

- This study found out that effective mitigation strategies for cybersecurity threats in cloud-based information systems at Kano Electricity Distribution Company involve the use of multi-factor authentication, encryption of sensitive data both in transit and at rest, deployment of intrusion detection and prevention systems, establishment of a comprehensive incident response plan, regular backups of critical data, and adherence to industry standards and regulations.

6. Conclusion

Effective cybersecurity management is critical for modern organizations, especially in safeguarding sensitive data, ensuring operational continuity, and maintaining stakeholder trust. This study has delved into evaluating cybersecurity practices within Kano Electricity Distribution Company (KEDCO), shedding light on key challenges and opportunities in cloud-based information security.

Organizations like KEDCO must acknowledge the paramount importance of cybersecurity and allocate resources towards robust strategies for identifying, mitigating, and managing cyber threats effectively. Training programs are essential for empowering employees with the requisite skills and knowledge to navigate cybersecurity challenges and leverage advanced technologies for enhanced threat detection and response.

Moreover, organizations should prioritize employee motivation and future prospects, fostering a culture of cybersecurity awareness and accountability across all levels. By nurturing a workforce that is adept at managing cybersecurity risks and staying abreast of emerging threats, KEDCO can strengthen its cybersecurity posture and protect critical assets from cyberattacks.

In conclusion, KEDCO stands to bolster its cybersecurity resilience and achieve its strategic objectives by prioritizing effective cybersecurity management, investing in continuous employee training and development, and fostering a culture of cybersecurity excellence. These concerted efforts will not only fortify KEDCO's defenses against cyber threats but also instill confidence among stakeholders and contribute to sustainable business growth and success in the digital age.

A. Recommendations

Based on the discussions, findings, and conclusions drawn from the study on cybersecurity in cloud-based information management at Kano Electricity Distribution Company (KEDCO), the following recommendations are proposed:

- KEDCO should allocate sufficient financial resources to support cybersecurity training and development initiatives for its employees. Investing in ongoing training programs will enhance employees' knowledge and skills in cybersecurity, contributing to improved threat detection, response, and decision-making processes within the organization's cloud-based information systems.
- KEDCO should enhance its human resource planning processes to ensure the recruitment and retention of qualified personnel with expertise in cybersecurity. By aligning workforce requirements with organizational cybersecurity goals, KEDCO can address staffing gaps and strengthen its capacity to manage cybersecurity risks effectively.
- Management at KEDCO should prioritize employees' future prospects by providing opportunities for career advancement, professional development, and succession planning in the cybersecurity domain. This will foster a motivated and skilled workforce capable of adapting to evolving cybersecurity challenges and contributing positively to organizational cybersecurity resilience.
- KEDCO should organize regular cybersecurity training and development programs for its staff, focusing on cybersecurity best practices, threat mitigation strategies, and emerging trends in cloud-based information security. By equipping employees with relevant cybersecurity knowledge and skills, KEDCO can enhance its cybersecurity capabilities and ensure alignment with industry standards and regulations.

References

[1]. Ahuja, V. (2000). Building trust in electronic commerce. IT Professional, 2(3), 61-63.

[2]. Bui, T., & Sivasankaran, T. R. (1987). Cost-effectiveness modeling for a decision support system in computer security. Computers & Security, 6(1), 139-151.

[3]. British Standards Institute. (1999). BS 7799: Information technology - Security techniques - Information security management. BSI.

[4]. Campbell, R. P., & Sands, G. A. (1979). A modular approach to computer security risk management. In AFIPS National Computer Conference (pp. 293-303).

[5]. Elmasri, R., & Navathe, S. B. (2004). Fundamentals of database systems (4th ed.). Addison Wesley.

[6]. Farahmand, F., Navathe, S. B., & Enslow, P. H. (2002, December). Electronic commerce and security—A management perspective. In ISS/INFORMS Seventh Annual Conference on Information Systems and Technology (San Jose, CA).

[7]. Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2003, September). Managing vulnerabilities of

information systems to security incidents. In ACM International Conference on Electronic Commerce, ICEC 2003 (Pittsburgh, PA).

[8]. Farahmand, F., Malik, W. J., Navathe, S. B., & Enslow, P. H. (2003). Security tailored to the needs of business. In ACM Workshop on Business-Driven Security Engineering (BIZSEC).

[9]. Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security (TISSEC), 4(3), 224-274.

[10]. Field, R. L. (1997). Issues in the law of electronic commerce. Networker (ACM Press), 1(3), 28-37.

[11]. Ghosh, A. K., & Swaminatha, T. M. (2001). Software security and privacy risks in mobile e-commerce. Communications of the ACM, 44(2), 51-57.

[12]. Henning, R. (1999, September). Security service level agreements: Quantifiable security for the enterprise? In ACM Proceedings of the 1999 Workshop on New Security Paradigm.

[13]. International Organization for Standardization. (1989). ISO 7498-2: Information processing systems—Open systems interconnection—Basic reference model—Part 2: Security architecture. ISO.

[14]. Joshi, J., et al. (2001). Security models for web-based applications. Communications of the ACM, 44(2), 38-44.

[15]. Landwehr, C. E., et al. (1993, November). A taxonomy of computer program security flaws, with examples. Naval Research Laboratory.

[16]. Landwehr, C. E., & Goldschlag, D. M. (1997). Security issues in networks with Internet access. In Proceedings of the IEEE (Vol. 85, No. 12, pp. 2034-2051).

[17]. Lindqvist, U., & Jonsson, E. (1997). How to systematically classify computer security intrusions. IEEE Symposium on Security and Privacy (pp. 154-163).

[18]. Lichtenstein, S. (1998). Internet risks for computers. Computers & Security, 17(2), 143-150.

[19]. Linketscher, N., & Child, M. (2001). Trust issues and user reactions to e-services and e-marketplaces: a customer survey. IEEE 12th International Workshop on Database and Expert Systems Applications (pp. 752).

[20]. Alshawi, S., Irani, Z., & Baldwin, L. (2003). Benchmarking information technology investment and benefits extraction. Benchmarking: An International Journal, 10(4), 423-432.

[21]. Baily, M. N., & Gordon, R. J. (1988). The Productivity Slowdown, Measurement Issues, and the Explosion of Computer Power. The American Economic Review, 78(2), 347-431.

[22]. Barua, A., Kriebel, C. H., & Mukhopadhyay, T. (1995). Information technologies and business value: An analytic and empirical investigation. Information Systems Research, 6(1), 3-18.

[23]. Bhardwaj, S., Jain, L., & Jain, S. (2010). Cloud Computing: A Study of Infrastructure as a Service (IAAS). International Journal of Engineering and Information Technology, 2(1), 60–63.

[24]. Brynjolfsson, E., & Hitt, L. (1996). Paradox Lost? Firm-level Evidence on the Returns to Information Systems Spending. Management Science, 42(4), 541-558.

[25]. Davenport, T. H., & Short, J. E. (1990). The New Industrial Engineering: Information Technology and Business Process Redesign. Sloan Management Review, 31(4), 11-27.

[26]. Dehning, B., & Stratopoulos, T. (2002). DuPont analysis of an IT-enabled competitive advantage. International Journal of Accounting Information Systems, 3(3), 165-176.

[27]. Hershey, P., & Silo, C. (2012). Procedure for detection of and response to distributed denial of service cyber-attacks on complex enterprise systems. In Proceedings of 6th Annual International Systems Conference (pp. 85-90). Vancouver, Canada.

[28]. Hitt, L. M., & Brynjolfsson, E. (1996). Productivity, Business Profitability, and Consumer Surplus: Three Different Measures of Information Technology Value. MIS Quarterly, 20(2), 121-142.

[29]. Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. Decision Support Systems, 51(1), 176–189.

[30]. Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. MIS Quarterly, 28(2), 283-322.

[31]. Microsoft (2014). Threat modeling tool.

[32]. Mooney, J. G., Gurbaxani, V., & Kraemer, K. L. (1996). A process-oriented framework for assessing the business value of information technology. ACM SIGMIS Database, 27(2), 68-81.

[33]. Motahari-Nezhad, H., Stephenson, B., & Singhal, S. (2009). Outsourcing Business to Cloud Computing Services: Opportunities and Challenges. LABs of HP.

[34]. National Institute of Standards and Technology Computer Security Division (2006). Guide for developing security plans for federal information systems, NIST SP 800-18 (Rev. 1).

[35]. Annesley, T. M. (2010). The discussion section: Your closing argument. Clinical Chemistry, 56(11), 1623-1628.

[36]. Bryman, A. (2016). Social research methods. Oxford University Press.

[37]. Bryman, A., & Bell, E. (2015). Business research methods. Oxford University Press.

[38]. Cohen, L., Manion, L., & Morrison, K. (2018). Research methods in education. Routledge.

[39]. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approach. Sage Publications.

[40]. Denzin, N. K., & Lincoln, Y. S. (2018). The SAGE Handbook of Qualitative Research. Sage Publications.

[41]. Hess, D. R. (2004). How to write an effective discussion. Respiratory Care, 49(10), 1134-1140.

[42]. Macoun, R. J. (1998). Biases in the interpretation and use of research results. Annual Review of Psychology, 49(1), 259-287.

[43]. Mohammed, A. (2015). Importance of survey research design: Quantitative and positivistic nature. Journal of Research Methods, 3(2), 45-58.
[44]. Neuman, W. L. (2014). Social research methods: Qualitative and quantitative approaches. Pearson.
[45]. Patton, M. Q. (2015). Qualitative research & evaluation methods: Integrating theory and practice. Sage Publications.
[46]. Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students. Pearson Education Limited.
[47]. Silverman, D. (2016). Qualitative research. Sage Publications.
[48]. Titchener, J., & Basturkmen, H. (2009). Perceptions of the difficulties of postgraduate L2 thesis students writing the discussion section. Journal of English for Academic Purposes, 8(1), 4-18.
[49]. Yin, R. K. (2018). Case study research and applications: Design and methods. Sage Publications.
[50]. Alao, D., Osah, G. and Eteete, A. (2019). Unabated Cyber Terrorism and Human Security Nigeria. Asian.
[51]. Osho, O. and Onoja, A. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. International Journal of cyber criminology, 9(1), pp.120–143.
[52]. Osho, O., Falaye, A. and Abdulhamid, S. (2013). Combating Terrorism with Cybersecurity: The Nigerian Perspective. World Journal of Computer Application and Technology, 1, pp.103–109.
[53]. Yakubu, M.A. (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, 7, pp.315–321.
[54]. Babayo, S., Muhammad, Y., Usman, S. and Bakri, M. (2021). Cybersecurity and Cybercrime in Nigeria: The Implications on National Security and Digital Economy. 4, pp.27–61.
[55]. Frank, I. and Odunayo, E. (2013). Approach to Cyber Security Issues in Nigeria: Challenges and Solution. International Journal of Cognitive Research in Science, Engineering and Education, 1(1), pp.100–110.
[56]. Ahuja, V. (2000). Building trust in electronic commerce. IT Professional, 2(3), 61-63.
[57]. Halder, D. and Jaishankar, K., (2011). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations: Laws, Rights and Regulations. Hershey, PA, USA: IGI Global.
[58]. Handler, S. and Rowley, L. (2022). The 5×5—Cybercrime and National Security. [online] Atlantic Council.