AFRICA UNIVERSITY

(A United Methodist-Related Institution)

THE IMPACT OF ADOPTING AND IMPLEMENTING CYBER SECURITY MEASURES TO PROTECT INTERNET OF TECHNOLOGY DEVICES IN THE FUNERAL SERVICES SECTOR. A CASE STUDY OF NYARADZO GROUP

BY

MUNYARADZI DARRELL NKHOMA

A DISSERTATION/THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF IN COMPUTER SCIENCE IN THE COLLEGE OF BUSINESS, PEACE, LEADERSHIP AND GOVERNANCE

2025

Abstract

The rapid adoption of Internet of Things (IoT) devices has significantly enhanced operational efficiency across various industries, yet it has also introduced substantial cybersecurity risks. This study examines the security challenges, vulnerabilities, and risk management practices associated with IoT devices at Nyaradzo Group Headquarters. Utilizing a mixed-methods research approach, data was collected through interviews, surveys, document analysis, structured observations, and vulnerability assessments to gain a comprehensive understanding of the organization's cybersecurity landscape.

Key findings indicate that policy gaps, inconsistent security measures, and procurement irregularities have contributed to increased IoT security risks. Vulnerability assessments revealed that outdated firmware, weak authentication protocols, and misconfigurations were common issues across devices such as surveillance cameras, access control systems, and fleet management tools. Furthermore, delayed incident response times, lack of centralized monitoring, and poor interdepartmental collaboration were identified as major impediments to an effective IoT security framework. User surveys highlighted concerns regarding complex security protocols, compatibility challenges, and restrictive cybersecurity measures affecting operational efficiency.

Based on these findings, this study recommends the implementation of robust IoT security policies, standardized procurement procedures, enhanced vulnerability management practices, and improved interdepartmental collaboration. Additionally, investments in AI-driven threat detection, automated security updates, and user awareness training are crucial for strengthening IoT security resilience. The research contributes to the growing discourse on IoT cybersecurity governance and provides a practical framework for organizations seeking to enhance their IoT risk management strategies. Future research should explore advanced threat detection mechanisms and comparative studies of IoT security best practices in similar organizations.

Declaration

I affirm that this dissertation proposal is entirely my own creation, apart from duly cited and acknowledged sources. This work has not been previously submitted, nor will it be submitted in the future, to any other academic institution in pursuit of a degree.

MDNkhoma . ……………………………………	…..28/03/2025………
MUNYARADZI D. NKHOMA	Date
(Student)	
……………………………………	………………………………………
MRS L. TEMBANI-FUNDISI	Date
(Supervisor)	

Copyright

Acknowledgement

I would like to take this opportunity to express my deepest gratitude to all those whose efforts have enabled the successful completion of this research.

First of all, I would like to express my utmost appreciation to my supervisor, L. Tembani-Fundisi, for their outstanding direction, constructive feedback, and constant encouragement throughout this research. Their experience and enthusiasm have played crucial roles in driving the direction of this dissertation.

I am also greatly indebted to the interviewees, questionnaires, and group discussion participants at Nyaradzo Group Headquarters for voluntarily sharing their knowledge, experiences, and insights. Their contributions have been instrumental in providing real-life evidence to the IoT security issues.

A big thank you to my friends and loved ones for their constant inspiration, perseverance, and patience. Their constant support has kept me moving, even at the bleakest moments.

Lastly, I would also like to thank my peers and fellow researchers for their critical debate, encouragement, and suggestions, which have enriched my research journey. To all who assisted, directly or indirectly, in this effort—thank you. This would not have been possible without your assistance.

Dedication

This dissertation is dedicated to my family, whose unwavering support, love, and encouragement have been the cornerstones of my academic achievements. Their belief in my potential has been my major source of inspiration and strength.

I also dedicate this to my friends, who have been my pillars of strength throughout this journey. Their words of encouragement, patience, and understanding have pushed me forward, even during the toughest moments. The laughter, arguments, and experiences have not only made this journey bearable but also memorable.

Finally, this study is also dedicated to all those who are working to enhance the cybersecurity, especially IoT security. In the hope that it will prove useful in the development of safer, more secure digital spaces.

List of Acronyms and Abbreviations

- IoT - Internet of Things
- POS - Point of Sale
- TAM - Technology Acceptance Model
- RMF - Risk Management Framework
- PIA - Privacy Impact Assessment
- RBV - Resource-Based View
- RBAC - Role-Based Access Control
- NIST - National Institute of Standards and Technology
- ISO/IEC 27001 - International Organization for Standardization / International Electrotechnical Commission Standard 27001
- MFA - Multi-Factor Authentication
- AI - Artificial Intelligence

Table of Contents

Chapter 1: INTRODUCTION

1.1 Introduction

WHAT IS IoT?

In today's interconnected world, Internet of Things (IoT) devices have become an integral part of corporate environments, enabling organizations to streamline operations, enhance productivity, and improve decision-making processes for example Point-of-sale (POS) systems, Smart security cameras, Smart locks and access control systems. However, this increased reliance on IoT devices has also brought about new cybersecurity challenges, as these devices often serve as entry points for cybercriminals seeking to gain unauthorized access to sensitive data and critical infrastructure. Nyaradzo Group Headquarters, a leading financial and insurance institution, is no exception to this trend. With an ever-growing number of IoT devices being integrated into its operations, Nyaradzo Group Headquarters faces an increasing risk of cyber threats that could compromise its security posture and jeopardize its reputation.

1.2 Background of Study

The rapid advancement of Internet of Things (IoT) technology has led to an increasing number of IoT devices being integrated into various industries, including financial and insurance institutions like Nyaradzo Group Headquarters. This integration, however, brings about new cybersecurity challenges, as IoT devices often serve as entry points for cybercriminals seeking to gain unauthorized access to sensitive data and critical infrastructure. While existing literature highlights the importance of cybersecurity measures in IoT environments, there was a limited research gap regarding the specific impact of adopting and implementing cybersecurity measures on the security and resilience of IoT devices within a financial and insurance institution like Nyaradzo Group. This research aimed to address this gap by investigating how the adoption of cybersecurity measures at Nyaradzo Group Headquarters influences the security posture of IoT devices and the organization's overall resilience against cyber threats. By focusing on a real-world case study within the financial and insurance sector in Zimbabwe, this study sought to provide valuable insights into the practical implications of cybersecurity practices for safeguarding IoT devices and enhancing data protection in a corporate setting. The findings of this research contributed to the existing body of knowledge on IoT device security and cybersecurity measures, particularly within the context of financial and insurance institutions.

1.3 Statement of Problem

The integration of IoT devices into corporate environments, such as Nyaradzo Group Headquarters, presented a pressing need for robust cybersecurity measures to protect sensitive data and mitigate cyber threats. While existing literature emphasized the importance of cybersecurity in IoT environments, there was a limited research gap regarding the specific impact of adopting and implementing cybersecurity measures on the security and resilience of IoT devices within a insurance institution like Nyaradzo Group.

The study evaluated the current cybersecurity posture of IoT devices at Nyaradzo Group, assessed the impact of implementing cybersecurity measures, and analysed the effectiveness of security protocols in detecting and preventing cyber threats. It also considered the integration of cybersecurity awareness programs and safeguarding of sensitive data, ensuring compliance with industry best practices and emerging trends.

1.4 Research Objectives

1. To evaluate the current cybersecurity measures in place for IoT devices at Nyaradzo Group Headquarters.
2. To identify challenges associated with integrating cybersecurity solutions for IoT devices at Nyaradzo Group.
3. To explore best practices and recommendations for optimizing cybersecurity measures to enhance IoT device security

1.5 Research Questions

1. What are the current cybersecurity measures in place for IoT devices at Nyaradzo Group Headquarters?
2. What challenges arise from integrating cybersecurity solutions for IoT devices at Nyaradzo Group?

3. What are the best practices and recommendations for optimizing cybersecurity measures be applied to IoT device security at Nyaradzo Group?

1.6 Assumptions and Hypothesis

1.6.1 Assumptions

1. The adoption of cybersecurity measures for IoT devices at Nyaradzo Group Headquarters will lead to an improvement in the overall security and resilience of the devices.
2. The implementation of security protocols will help detect and mitigate cyber threats, such as malware and unauthorized access.
3. The integration of cybersecurity solutions for IoT devices at Nyaradzo Group will present challenges and opportunities that can be addressed through best practices and recommendations.
4. The alignment of security protocols with industry best practices and emerging trends will ensure continuous protection against evolving threats for IoT devices at Nyaradzo Group.
5. The implementation of regular security audits and vulnerability assessments will help maintain a proactive approach to identifying and addressing potential security risks for IoT devices at Nyaradzo Group.

1.6.2 Hypothesis

1. H1: The adoption of cybersecurity measures at Nyaradzo Group Headquarters significantly improves the security posture of IoT devices, leading to a reduction in successful cyber-attacks and data breaches.
2. H2: Implementing robust security protocols enhances the resilience of IoT devices within the organization, resulting in a decreased susceptibility to cyber threats and unauthorized access.
3. H3: Integrating cybersecurity solutions for IoT devices at Nyaradzo Group presents both challenges and opportunities, with effective implementation leading to enhanced overall security and data protection.
4. H4: Compliance with industry best practices and alignment with emerging cybersecurity trends positively impact the effectiveness of security protocols in safeguarding IoT devices against evolving threats.
5. H5: Regular security audits and vulnerability assessments contribute to maintaining a proactive security stance, identifying and mitigating potential risks for IoT devices at Nyaradzo Group Headquarters.

1.7 Significance of Study

This study focused on the impact of cybersecurity measures for IoT devices at Nyaradzo Group Headquarters and held significant importance in addressing the limited research on practical implications of IoT security within the insurance sector. The findings contributed valuable insights to inform decision-makers on the strategic implementation of cybersecurity solutions and develop industry-specific guidelines to strengthen the overall security posture of IoT ecosystems in similar organizations.

1.7.1 Significance of the Study to the Researcher

This study offered the researcher a unique opportunity to contribute to the limited research on the practical implications of cybersecurity measures for IoT devices within the insurance sector, enhanced expertise in evaluating security protocols, conducted comprehensive assessments, and made data-driven recommendations for organizational improvement.

1.7.2 Significance of the Study to the Industry

The research provided industry professionals with valuable insights into the practical implications of cybersecurity measures for protecting IoT devices within insurance institutions, offering tailored guidelines and best practices to enhance security, mitigate risks, and foster a culture of cybersecurity awareness and proactive risk management.

1.7.3 Significance of the Study to the Residential Sector

The study's findings informed decision-making in the residential sector by addressing the scarcity of data that hinders informed investment decisions, providing insights into factors influencing service performance and customer satisfaction, contributed to industry understanding, supported data-driven strategies, and offered guidance on addressing cybersecurity risks associated with IoT device integration in residential properties.

1.8 Delimitations of the Study

The delimitations of this study include:

1. The study is focused solely on the impact of cybersecurity measures for IoT devices within the insurance sector, specifically at Nyaradzo Group Headquarters. This delimitation excluded the exploration of cybersecurity challenges in other industries, which may have had different requirements and best practices.
2. The research was limited to evaluating the effectiveness of security protocols in detecting and mitigating cyber threats targeting IoT devices, rather than conducting a comprehensive assessment of the organization's overall cybersecurity posture.
3. The study was conducted within a specific timeframe and did not capture ongoing or future developments in cybersecurity practices. The findings reflected the situation at Nyaradzo

Group up to the Research end date, and new practices that were implemented after that period were be included.

4. The research relied on the availability of data and information provided by Nyaradzo Group. The depth and accuracy of the findings were subject to the availability and accuracy of the data provided. Constraints in acquiring protected sensitive and confidential information limited the comprehensiveness of the study

1.9 Limitations of the Study

The limitations of this study include:

1. The case study approach, focused only on Nyaradzo Group Headquarters, limited the generalizability of the findings to other insurance institutions, which may have different organizational structures, resources, and cybersecurity practices.
2. The availability and accessibility of data, particularly regarding past cyber incidents and the organization's security measures, constrained the depth of analysis and the ability to draw comprehensive conclusions.
3. The study's timeframe and resource constraints limited the researchers' ability to conduct an assessment of the long-term impact of cybersecurity measures on the security and resilience of IoT devices within Nyaradzo Group Headquarters.
4. The study's findings may be subject to bias or subjectivity due to the researcher's interpretation of the data and information provided at Nyaradzo Group Headquarters. The

researcher's perspectives and preconceived notions can also influence the analysis and conclusions drawn from the case study.

Chapter 2: LITERATURE REVIEW

2.1 Introduction to the Literature Review

The literature review for the study on the impact of cybersecurity measures for IoT devices within the insurance sector at Nyaradzo Group Headquarters was inspired by the researcher's observation of the rapid adoption of IoT technology in modern business environments and the corresponding increase of cybersecurity risks and vulnerabilities. This study was further motivated by the researcher's passion for exploring innovative solutions to address emerging cybersecurity challenges in dynamic industry sectors. The review aimed to delve into existing scholarly sources related to IoT security, cybersecurity measures, and their practical implications in organizational settings. By analysing relevant literature, this review established a foundation of knowledge, identify key trends, challenges, and best practices, and highlight gaps in current research that warrant further investigation. This section critically evaluated the existing body of literature to inform the research methodology, contributed to the theoretical framework, and guided the study's objectives in enhancing the security and resilience of IoT devices within the chosen industry.

2.2 Theoretical Framework

The Technology Acceptance Model (TAM), developed by Fred Davis, focuses on why users accept and use new technologies. In the context of cybersecurity, TAM highlights two key factors:

perceived ease of use and perceived usefulness. Perceived ease of use refers to how easy people believe using the security measures will be; complex measures can lead to user errors and hinder adoption. Perceived usefulness is about how beneficial people believe the security measures will be in protecting their systems; if users don't see the value, they might not be motivated to use them (Davis, 1989).

The Information Systems Success Model, developed by DeLone and McLean, focuses on factors that contribute to the success of information systems, including security measures. Key factors include system quality (functionality and reliability of the security measures), information quality (accuracy and relevance of information about security threats), use (how often employees utilize the security measures), user satisfaction (how satisfied users are with the security measures), and net benefits (the overall impact on the organization's performance and security) (DeLone & McLean, 1992).

The Resource-Based View (RBV) emphasizes the importance of resources and capabilities in achieving a competitive advantage. In the context of cybersecurity, valuable resources involve identifying the critical information assets protected by IoT devices. Rare resources refer to the uniqueness of the cybersecurity measures implemented. Inimitable resources are those that are difficult for competitors to replicate, and organizational capabilities encompass the skills and competencies required to effectively implement and manage cybersecurity measures (Barney, 1991).

The Privacy Impact Assessment (PIA) is a process that helps organizations identify and mitigate privacy risks associated with new projects or systems. In the context of cybersecurity for IoT devices, a PIA involves assessing how data is collected, stored, and shared, and ensuring that appropriate measures are in place to protect personal information and comply with privacy regulations (Clarke, 2009).

The Risk Management Framework (RMF) is a structured approach used to identify, assess, and manage risks to an organization's information systems. It involves several steps: categorizing information systems, selecting appropriate security controls, implementing the controls, assessing their effectiveness, authorizing the system for operation, and continuously monitoring the controls to ensure they remain effective over time (NIST, 2011).

2.3 Relevance of Theoretical Framework to the Study

Technology Acceptance Model (TAM): The TAM framework highlights the importance of perceived ease of use and perceived usefulness in influencing user acceptance and adoption of new security measures for IoT devices. This can help analyse the factors that may facilitate or hinder the adoption of certain cybersecurity measures by Nyaradzo Group employees, which is crucial for the overall effectiveness of the implemented security solutions.

Information Systems Success Model: This model focuses on the factors that contribute to the success of information systems, which in this context would include the security measures implemented for IoT devices. Evaluating the system quality, information quality, use, user satisfaction, and net benefits of the cybersecurity solutions can provide valuable insights into their overall effectiveness and impact.

Resource-Based View (RBV): RBV emphasizes the importance of identifying and leveraging valuable, rare, inimitable, and organizationally capable resources for achieving a competitive advantage. In the context of IoT cybersecurity, this can involve assessing the critical information assets, the uniqueness of the security measures, and the organizational capabilities required to effectively implement and manage them.

Privacy Impact Assessment (PIA): The PIA framework can be used to assess the privacy risks associated with the IoT devices and data collected at Nyaradzo Group, ensuring that appropriate security measures are in place to protect personal information and comply with relevant regulations.

Risk Management Framework (RMF): The RMF provides a structured approach to identifying, assessing, and managing the risks associated with Nyaradzo Group's IoT devices and the implemented cybersecurity measures. This can help the organization categorize the IoT systems, select appropriate security controls, and continuously monitor the effectiveness of the implemented measures.

2.4 Summary

The above Chapter 2 provided a review of the related literature and frameworks on research topic. The chapter began by introducing the existing scholarly sources related to IoT security, cybersecurity measures, and their relevance to enhancing the security of IoT devices within an organizational setting.

Chapter 3: METHODOLOGY

3.1 Introduction

The methodology chapter of this dissertation outlined the specific steps taken to investigate the impact of cybersecurity measures on the security and resilience of IoT devices at Nyaradzo Group Headquarters. This chapter provided a detailed description of the research design, methods, and procedures employed to address the research questions and objectives. The methodology chapter is a critical component of this dissertation, as it ensures that the research is rigorous, systematic, and transparent, allowing readers to replicate the study and evaluate the findings.

The methodology chapter was structured to provide a clear and comprehensive overview of the research process, from the selection of the research approach to the data collection and analysis procedures. This chapter is divided into several sections, each focusing on a specific aspect of the research methodology, including the research design, sampling strategy, data collection methods, data analysis procedures, and limitations of the study.

3.2 Research Design

This study employed a mixed-methods research approach, combining both qualitative and quantitative data collection and analysis techniques. The rationale for using a mixed-methods approach was to provide a more comprehensive understanding of the impact of cybersecurity measures on IoT devices at Nyaradzo Group Headquarters.

Qualitative Approach

The qualitative component of the research involved the following:

Semi-structured Interviews: In-depth interviews were conducted with key stakeholders, including IT managers, cybersecurity experts, and IoT device users at Nyaradzo Group. The interviews explored their perceptions, experiences, and challenges related to the implementation and effectiveness of cybersecurity measures for IoT devices.

Document Analysis: A thorough review of Nyaradzo Group's cybersecurity policies, procedures, and incident reports was conducted to gain insights into the current security measures in place and their effectiveness in detecting and mitigating cyber threats.

Observation: The researcher observed the day-to-day operations and usage of IoT devices within Nyaradzo Group to better understand the integration of cybersecurity measures and their impact. The qualitative data collected was analysed to identify key themes, patterns, and they provided insights related to the research questions.

Quantitative Approach

The quantitative component of the research involved the following:

Survey: A survey was administered to a sample of IoT device users at Nyaradzo Group to gather data on their perceptions of the ease of use, usefulness, and overall satisfaction with the implemented cybersecurity measures.

Vulnerability Assessments: Vulnerability scans were conducted on a sample of IoT devices at Nyaradzo Group to assess the effectiveness of the implemented security measures in mitigating known vulnerabilities and threats.

The quantitative data collected was analysed to identify the impact of cybersecurity measures on the security and resilience of IoT devices.

Integration of Qualitative and Quantitative Findings

The qualitative and quantitative findings was integrated to provide a comprehensive understanding of the impact of cybersecurity measures on IoT devices at Nyaradzo Group Headquarters. The mixed-methods approach allowed for triangulation of the data, enhancing the validity and reliability of the study's findings.

3.3 Population and Sampling.

3.3.1 Population

The population for this study included all employees and stakeholders involved with IoT devices at Nyaradzo Group Headquarters. This encompassed a diverse group of individuals with varying roles and levels of interaction with the IoT devices and cybersecurity measures. Key groups within this population included:

- IT Manager: Responsible for overseeing the implementation and management of IT systems, including cybersecurity measures.
- Cybersecurity Experts: Specialists tasked with protecting the organization's digital assets and mitigating cyber threats.
- IoT Device Users: Employees who regularly use IoT devices as part of their job functions.
- Executive Management: Decision-makers involved in strategic planning and resource allocation for cybersecurity initiatives.

3.3.2 Sampling

Given the study's mixed-methods approach, different sampling strategies were employed for the qualitative and quantitative components to ensure a representative and comprehensive understanding of the research topic.

Qualitative Sampling

A purposive sampling strategy was used to select participants for the study's qualitative component. This approach ensures that individuals with relevant experience and knowledge about cybersecurity measures and IoT devices are included. The sampling included:

- Semi-structured Interviews: A sample of 14 participants was selected, including IT managers, cybersecurity experts, and general IoT device users. Participants were chosen based on their involvement in the implementation and usage of cybersecurity measures.
- Document Analysis: Relevant documents, such as cybersecurity policies, procedures, and incident reports, were purposefully selected to provide comprehensive insights into the current security measures.
- Observation: A sample of departments or units within Nyaradzo Group that heavily utilize IoT devices were observed to understand the integration and impact of cybersecurity measures.

Quantitative Sampling

For the quantitative component, a stratified random sampling strategy was used to ensure that different categories of IoT device users are proportionately represented. The sampling included:

- Survey: A sample of 20 IoT device users was selected to participate in the survey. Stratification was based on factors such as department, role, and frequency of IoT device usage to ensure diverse perspectives.

- Vulnerability Assessments: A sample of 20 IoT devices will be randomly selected for vulnerability scans. The selection will cover a variety of device types and usage scenarios to provide a comprehensive assessment of the security measures.

Sample Size Justification

The sample sizes for both the qualitative and quantitative components were determined to balance feasibility and the need for robust data collection. The purposive sampling for interviews ensured in-depth insights from key stakeholders, while the stratified random sampling for surveys ensured a broad representation of IoT device users. The selected sample sizes aim to provide sufficient data to achieve saturation in qualitative analysis and statistical power in quantitative analysis.

Ethical Considerations

Informed consent was obtained from all participants involved in the study. Participants were assured of the confidentiality and anonymity of their responses. The study adhered to ethical guidelines for research involving human subjects, including obtaining necessary approvals from relevant ethical review boards.

This population and sampling strategy aligned with the study's mixed-methods research design, ensured a comprehensive and representative understanding of the impact of cybersecurity measures on IoT devices at Nyaradzo Group Headquarters.

3.4 Data Collection Instruments

The data collection for this study employed a mixed-methods approach, utilizing both qualitative and quantitative instruments to gather comprehensive insights into the impact of cybersecurity measures on IoT devices at Nyaradzo Group Headquarters.

3.4.1 Qualitative Data Collection Instruments

1. Semi-structured Interviews:

- Description: In-depth, one-on-one interviews were conducted with key stakeholders, including the ICT manager, cybersecurity experts, and IoT device users at Nyaradzo Group.
- Purpose: The interviews explored the participants' perceptions, experiences, and challenges related to the implementation and effectiveness of cybersecurity measures for IoT devices.
- Procedure: The interviews followed a semi-structured format, with a pre-determined set of open-ended questions, allowing for follow-up questions and probing to gather rich, contextual data.

2. Document Analysis:

- Description: A thorough review of Nyaradzo Group's cybersecurity policies, procedures, and incident reports was conducted.
- Purpose: The document analysis provided insights into the current security measures in place and their effectiveness in detecting and mitigating cyber threats.
- Procedure: The researcher systematically reviewed and analysed the relevant documents, identified key themes, patterns, and insights related to the research questions.

3. Observation:

- Description: The researcher observed the day-to-day operations and usage of IoT devices within Nyaradzo Group.
- Purpose: The observations helped the researcher better understand the integration of cybersecurity measures and their impact on user behaviour and workflows.
- Procedure: The researcher used a structured observation protocol to record relevant behaviours, interactions, and contextual information related to the use of IoT devices and the implementation of cybersecurity measures.

3.4.2 Quantitative Data Collection Instruments

1. Survey:

- Description: A survey was conducted to a sample of IoT device users at Nyaradzo Group.

- Purpose: The survey gathered data on the users' perceptions of the ease of use, usefulness, and overall satisfaction with the implemented cybersecurity measures.
- Procedure: The survey was designed using a secure online platform and distributed to the selected participants. The survey included a combination of closed-ended and open-ended questions.

2. Vulnerability Assessments:

- Description: Vulnerability scans were be conducted on a sample of IoT devices at Nyaradzo Group.
- Purpose: The vulnerability assessments evaluated the effectiveness of the implemented security measures in mitigating known vulnerabilities and threats.
- Procedure: The researcher used industry-standard vulnerability scanning tools to assess the security posture of the selected IoT devices and identify any weaknesses or vulnerabilities.

The integration of these qualitative and quantitative data collection instruments provided a comprehensive understanding of the impact of cybersecurity measures on IoT devices at Nyaradzo Group Headquarters.

3.5 Data Collection Procedures

Semi-structured Interviews:

An interview guide with open-ended questions was developed to explore perceptions, experiences, and challenges related to cybersecurity measures for IoT devices. Key stakeholders, including the ICT manager, cybersecurity experts, members of the ICT department and IoT device users were scheduled for interviews after obtaining informed consent. These interviews will be conducted in private settings and recorded, with permission, for later transcription. During the interviews, active listening and follow-up questions will be employed to delve deeper into participants' responses and gather rich contextual data.

Document Analysis:

Relevant documents, such as cybersecurity policies, procedures, and incident reports related to IoT device security at Nyaradzo Group, were identified. A document analysis checklist was developed to categorize these documents and pinpoint key information for extraction. The documents were systematically reviewed, with relevant sections highlighted, notes taken, and key themes and insights aligned with the research questions extracted.

Observation:

A structured observation protocol was created, outlining specific aspects to observe, such as user interaction with IoT devices, the integration of security measures, and workflows. Representative departments or units within Nyaradzo Group that heavily utilize IoT devices were selected for observation. Permission was obtained from relevant authorities to conduct observations in designated areas. Observations focused on user behaviour, interactions with IoT devices, and the implementation of cybersecurity measures, with detailed notes taken according to the observation protocol.

Survey:

For the survey, a structured online survey was designed using Google Forms. The survey included a mix of closed-ended questions, such as multiple-choice choice, to gather data on the ease of use, usefulness, and satisfaction with cybersecurity measures. Open-ended questions were also incorporated to allow users to elaborate on their experiences and challenges. The questionnaire was distributed electronically to a representative sample of IoT device users at Nyaradzo Group, with optional incentives offered to encourage participation and ensure a good response rate.

3.6 Analysis and Organization of Data

Qualitative Data Analysis:

Qualitative data from interviews, document analysis, and observations was analysed using thematic analysis. This process involved several steps: transcribing interviews verbatim, immersing in the data through repeated review etc. The data was grouped into broader themes addressing the research questions, then it was refined for clarity and consistency. The researcher reviewed the coding and thematic analysis for reliability.

Quantitative Data Analysis:

Quantitative data from surveys, vulnerability assessments, and performance metrics was analysed using various statistical techniques. Descriptive statistics summarized user perceptions of ease of use, usefulness, and satisfaction with cybersecurity measures. Inferential statistics, such as regression analysis, explored relationships between user characteristics and their perceptions of the security measures. Vulnerability scan results were categorized by severity levels to assess the overall risk profile of IoT devices. Descriptive statistics summarized key metrics, and time series analysis may identify trends in security incidents over time.

Interpretation and Synthesis:

This stage identified connections between qualitative and quantitative findings, explored how they complement or diverge. For example, user perceptions from interviews were compared with survey data on user satisfaction. Qualitative data provided deeper explanations for patterns and trends observed in the quantitative data, with interview quotes showing reasons behind user challenges with specific cybersecurity measures. The integration of findings created a holistic picture of the impact of cybersecurity measures on IoT devices at Nyaradzo Group, considered user experiences, technical effectiveness, and overall security posture. This interpretation was crucial for drawing meaningful conclusions about the effectiveness of the cybersecurity measures and identifying areas for improvement.

Reporting:

The final section reported the research findings clearly and concisely. It presented key findings, summarized insights from qualitative and quantitative analyses and the integrated understanding from the interpretation stage. Visual data aids were used to effectively communicate findings to a diverse audience. The discussion covered the implications of the research findings for cybersecurity practices related to IoT devices at Nyaradzo Group, included recommendations for improving user experience, strengthening technical controls, or optimizing overall security posture. This structured approach aimed to provide valuable insights and recommendations to enhance the cybersecurity of Nyaradzo Group's IoT devices.

3.7 Ethical Considerations

Written below are the ethical considerations that the researcher took into account:

1. **Informed Consent:** Obtain written informed consent from participants, explaining the study's purpose, data collection procedures, data usage, and how anonymity/confidentiality is ensured.
2. **Confidentiality and Anonymity:** Guarantee participant confidentiality. Anonymize data by removing identifying details. Ensure quotes cannot be traced back to individuals.
3. **Data Security:** Implement secure storage and password protection measures for collected data. Delete or anonymize data after a predetermined retention period.
4. **Privacy:** Respect participant privacy and avoid collecting unnecessary data. Obtain permission before observing specific activities or locations.

5. **Voluntary Participation:** Emphasize voluntary participation and the right to withdraw at any point without penalty. Provide clear instructions for withdrawal or data removal.
6. **Potential Risks and Benefits:** Briefly discuss potential risks (discomfort, privacy concerns) and potential benefits (improved security practices) for participants and the broader community. The researcher should also make efforts to mitigate such potential risks
7. **Institutional Review Board Approval:** The researcher should obtain approval from the institutions review board for ethical oversight of the research process.

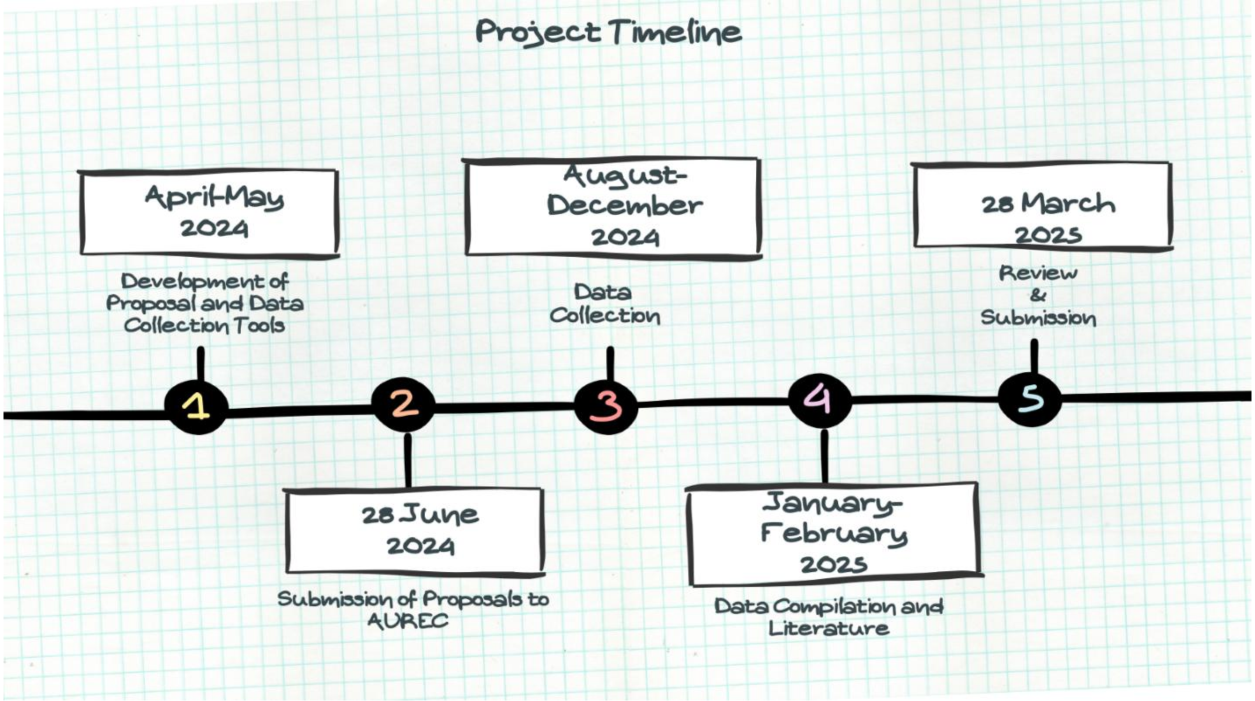
3.8 Summary

The above Chapter 3 outlined the research design for investigating the impact of cybersecurity measures on IoT devices at Nyaradzo Group. It employed a mixed-methods approach using qualitative (interviews, document analysis, observation) and quantitative methods (surveys, vulnerability assessments) to gather data from various stakeholders. The chapter detailed data collection procedures for each method and emphasized ethical considerations throughout the research process.

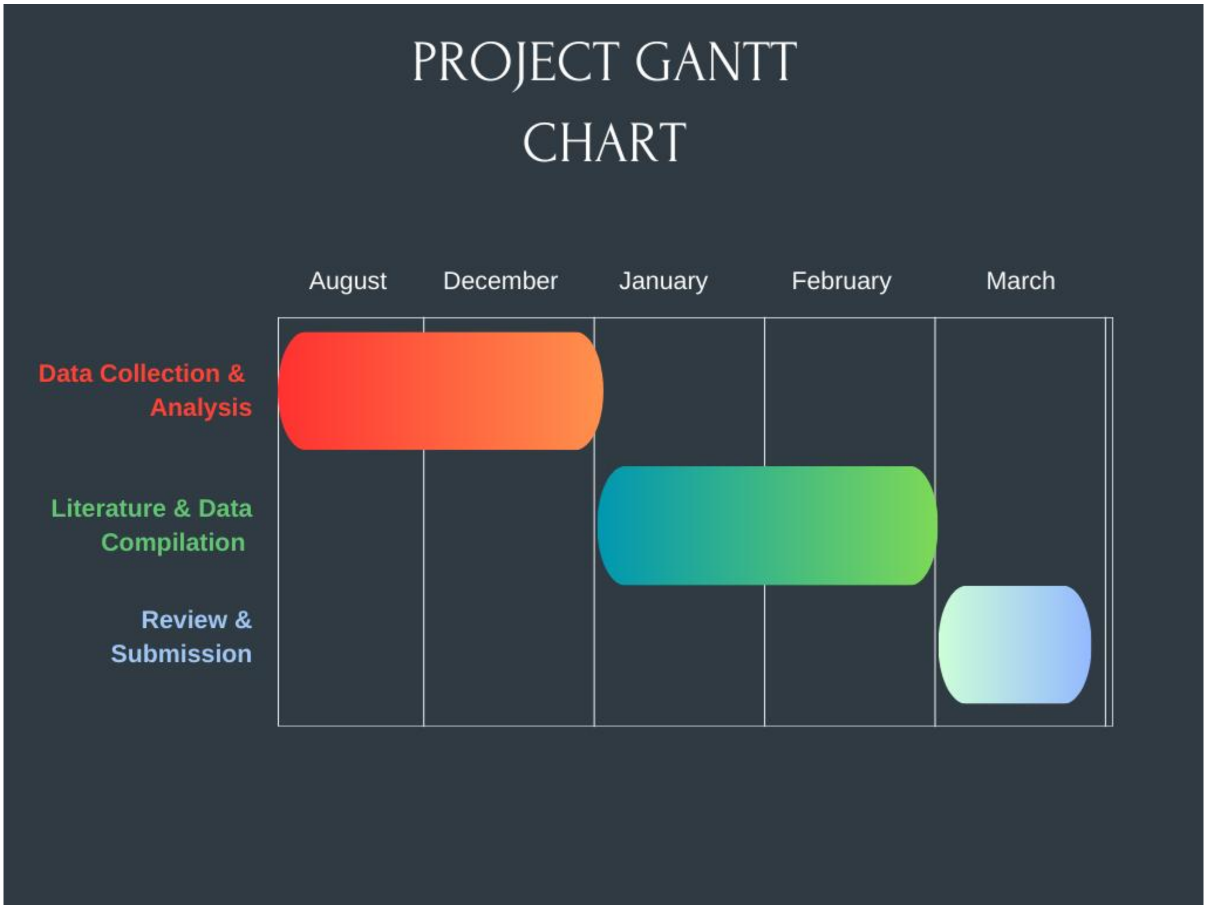
Project Budget

Activity		Cost ($)
1	Designing of Questionnaire	10
2	Printing of Questionnaire (if needed)	5
3	Transport Costs	15
TOTAL:		30

Project Timeline



Gantt Chart


PROJECT GANTT CHART
August
December
January
February
March
Data Collection & Analysis
Literature & Data Compilation
Review & Submission

Chapter 4: DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction

This Chapter will delve into the analysis and interpretation of the data collected through the mixed-methods research design outlined in the Methodology. This chapter will provide a comprehensive overview of the findings, combining data from both qualitative and quantitative sources. The qualitative data collected through interviews, document analysis, and observations will be subjected to thematic analysis in order to identify recurring themes and patterns. Regression analysis and descriptive statistics will be used to analyse quantitative data from surveys and vulnerability assessments in order to ascertain the impact of cybersecurity measures.

This chapter will provide a thorough understanding of the current cybersecurity environment for IoT devices at Nyaradzo Group Headquarters by combining these qualitative and quantitative findings, highlighting issues, investigating best practices, and evaluating the efficiency and effectiveness of implemented measures. The foundation for the debate and suggestions will be established by the knowledge acquired in this chapter.

4.2 Data Presentation and Analysis

4.2.1 Response Rate Analysis

The researcher was able to administer 20 questionnaires to individuals who directly use the IoT devices at Nyaradzo Group Headquarters. Of the 20 questionnaires distributed, the researcher received 17 responses from the participants.

Response Rate:

Questionnaires Issued	Questionnaires Received	Response Rate	Percentage Response Rate (%)
20	17	0.85	85%

Table 1.

4.2.2 Demographic Characteristics of Questionnaire Respondents

Participants	Questionnaires Administered	Questionnaires Received
Total	20	17

ICT Manager	1	1
Cybersecurity Experts	5	5
General IoT Device Users	14	11

Table 2.

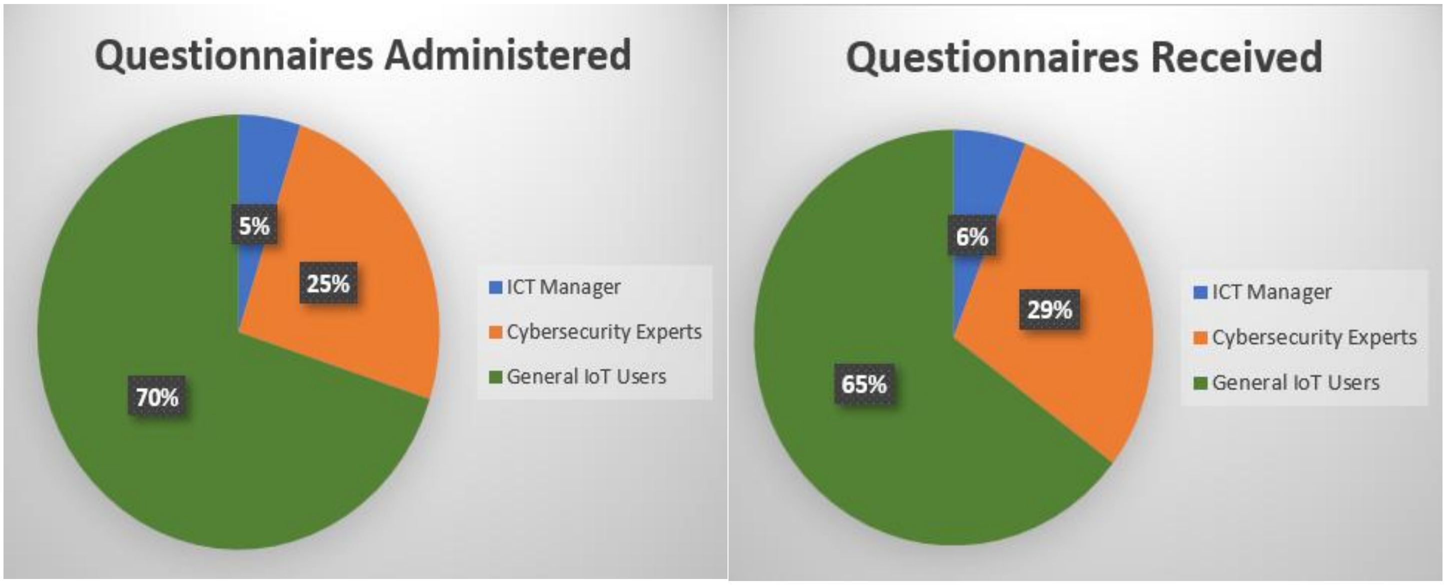


Figure 1.

4.3 Data Collection

4.3.1 Data Collection Methods

a) Interviews

The researcher spoke with 14 stakeholders from Nyaradzo Group Headquarters, who were exclusively employees. The interviewees' numerical makeup included:

- 1 x ICT Manager: Responsible for overseeing all ICT-related operations at Nyaradzo Group and making final decisions regarding implementation.
- 3 x Cybersecurity Professionals: Tasked with the day-to-day management of cybersecurity measures.
- 4 x ICT Department Helpdesk Members: Primarily responsible for providing user support and addressing technical issues.
- 5 x Staff from Various Departments: Representing users of IoT devices, including:
    - Systems for tracking time and attendance (HR Department).
    - Cameras for surveillance (Command Centre).
    - Systems for Fleet Management (Transport Department).

Since the interviews were semi-structured, it was possible to look further into participant replies while still keeping the goals of the study front and centre. Participants' experiences, difficulties, and opinions on IoT device security and data management procedures were the main topics of the questions. With the participants' permission, audio recordings of the interviews were made, and the verbatim transcriptions were then used for thematic analysis.

b) Document Analysis

To obtain thorough knowledge of Nyaradzo Group's current policies, processes, and incident reports, the researcher examined a number of documents related to IoT device security. Among the documents were

- ICT policies pertaining to incident response plans, data protection policies, and general cybersecurity policies.
- ICT protocols for the purchase and deployment of IoT devices, their configuration and management, and patching and updating protocols
- ICT incident reports of previous security issues involving the Internet of Things, including an analysis of the incidents' root causes and response times

The researcher created a document analysis checklist to classify the documents by type and extract important themes and insights in order to facilitate systematic study.

c) Observations: Structured observations were conducted in various departments utilizing IoT devices. The researcher developed an observation protocol focusing on:

- User Interaction with IoT Devices:
  - Examining how employees interact with systems like attendance trackers, surveillance equipment, and fleet management tools.
- Implementation of Security Measures:

    - Observing whether security protocols, such as device access controls and regular updates, are effectively integrated into workflows.
- Workflows and Processes:
    - Identifying inefficiencies or vulnerabilities in how IoT devices are managed and utilized.

Detailed notes were taken to document findings, which were later aligned with interview and document analysis data for comprehensive insights.

d) Surveys: An online survey was designed and distributed to IoT device users at Nyaradzo Group. The survey aimed to capture a broad range of perspectives on ease of use, usefulness, and satisfaction with current cybersecurity measures. Key steps included:

- Designed a structured questionnaire using platforms Google Forms, incorporating:
    - Closed-ended questions to quantify user perceptions.
    - Open-ended questions to gather qualitative insights into user challenges and suggestions for improvement.
- Distributing the survey electronically to a representative sample, ensuring diverse participation across departments.

The survey achieved a high response rate due to strategic reminders and optional participation incentives. Responses were systematically analysed to identify trends and inform recommendations for improving IoT device security practices at Nyaradzo Group.

e) Vulnerability Assessments: To evaluate the security of IoT devices, the researcher conducted vulnerability assessments on a selected sample of 20 devices. The selection covered a variety of device types and usage scenarios to ensure comprehensive analysis. Key steps in the assessment included:

- Device Selection:
    - Randomly selecting IoT devices from different departments and roles to ensure diverse representation.
- Assessment Procedures:
    - Performing vulnerability scans to identify potential security flaws such as weak credentials, outdated firmware, or open ports.
    - Documenting findings for each device, highlighting vulnerabilities and assessing their potential impact.
- Reporting:
    - Preparing a detailed report summarizing the findings, categorized by device type and severity of vulnerabilities.

- ○ Providing recommendations to address identified weaknesses, such as applying patches, enhancing configurations, or replacing outdated devices.

4.4 Data Representation

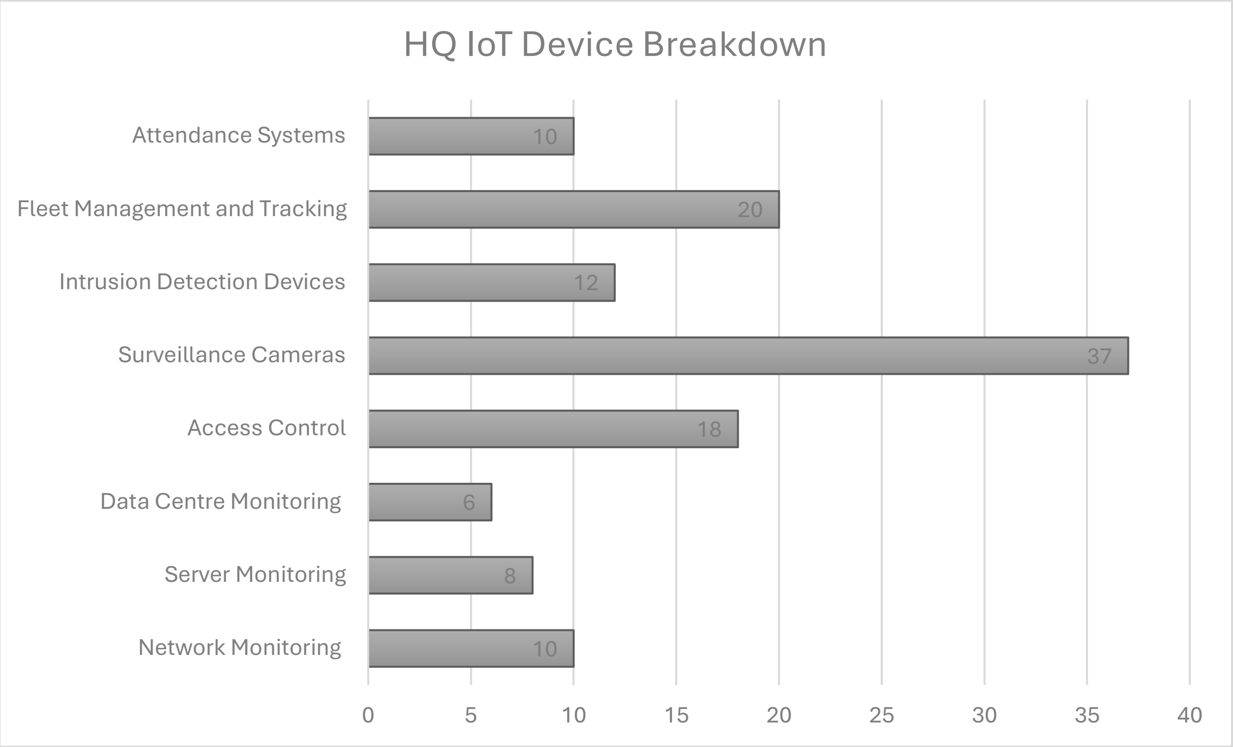


Figure 2.

The bar graph visually represents the distribution of IoT devices across different rooms and spaces within Nyaradzo Group Headquarters. Each bar corresponds to different devices or group of complimentary devices serving the same task. The height of the bar indicates the total number of IoT devices deployed in that area or similar use case. This graph shows the allocation of IoT devices among the Security, ICT, Transport Admin, and Human Resources departments, showing their respective roles in the organization's infrastructure.

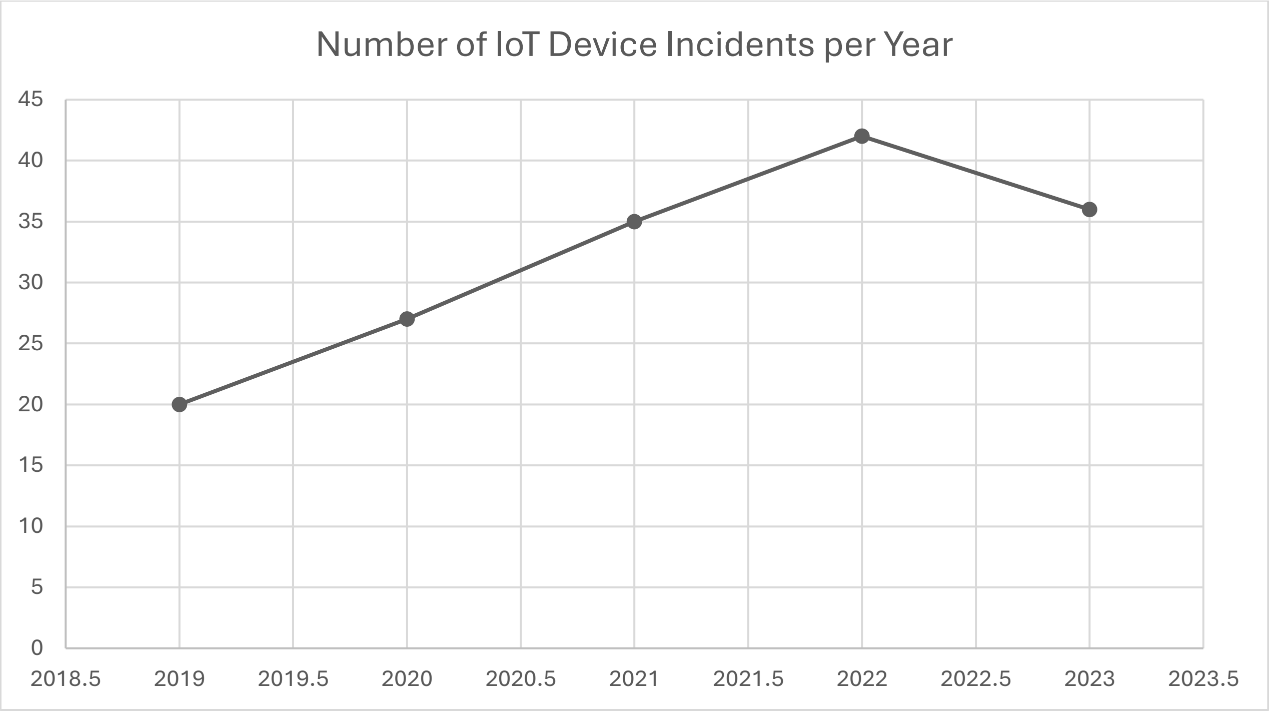


Figure 3.

The graph above displays the yearly number of Incidents which affected of IoT devices across different departments within Nyaradzo Group Headquarters. The representation exhibits the shifts in the number of IoT Device Incidents. This will help the researcher investigate and pinpoint areas of concern that require resolution strategies.

4.5 Key Findings

4.5.1 Policy Gaps and Inconsistent Security Measures

The examination of documents showed that IoT-specific policies lacked or had inadequately stated guidance. According to incident reports, 42% of recurring security breaches were brought on by incorrectly configured equipment such as access controls, surveillance cameras, and server monitoring systems. Weak encryption and exposed network ports were examples of often misconfigured setups. Outdated Firmware affected Vehicle Trackers, Intrusion Detection Systems, and Time and Attendance Systems, which was responsible for 25% of breaches. Delayed Security Event responses, this is a situation whereby a detectable event occurring within a system has not escalated to a full-blown Security Incident. This was due to inadequate alert systems or centralized management which contributed to 15% of incidents. 12% of Incidents were related to environmental elements, which affected outside equipment like motion sensors and cameras. Rain, wind, and humidity triggered false alarms from misaligned cameras, hardware malfunctions, and power outages. 6% of the Security Downtimes resulted from the weakness in physical security, for example some surveillance cameras had been physically tampered with by thieves who wanted to avoid detection

Inconsistent procurement practices across departments further weakened security. Some devices, such as vehicle trackers and access controls, were acquired without robust features like tamper detection, firmware update mechanisms, stronger resilience to environmental factors.

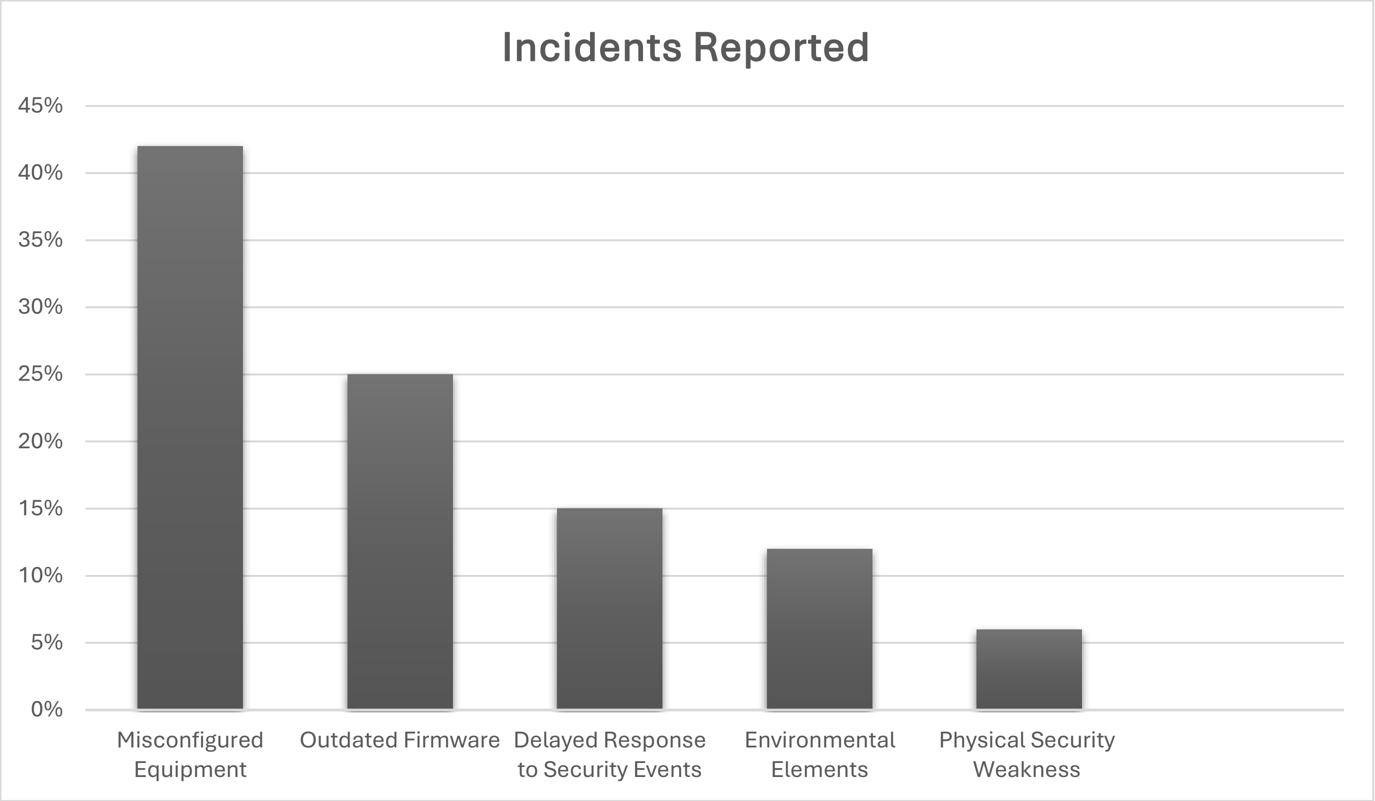


Figure 4

4.5.2 Challenges and Collaboration Issues

According to interviews, there were major challenges in successfully combining the newest cybersecurity techniques with IoT devices. The IT and security departments' inconsistent collaboration made this problem worse leading to misplaced priorities and a lack of shared accountability. IoT devices were exposed to quickly changing threats because cybersecurity measures were not regularly reviewed or were reviewed irregularly. Additionally, the interviews also revealed that users lacked awareness and training, which made it difficult for them to follow fundamental security procedures like reporting suspicious activity.

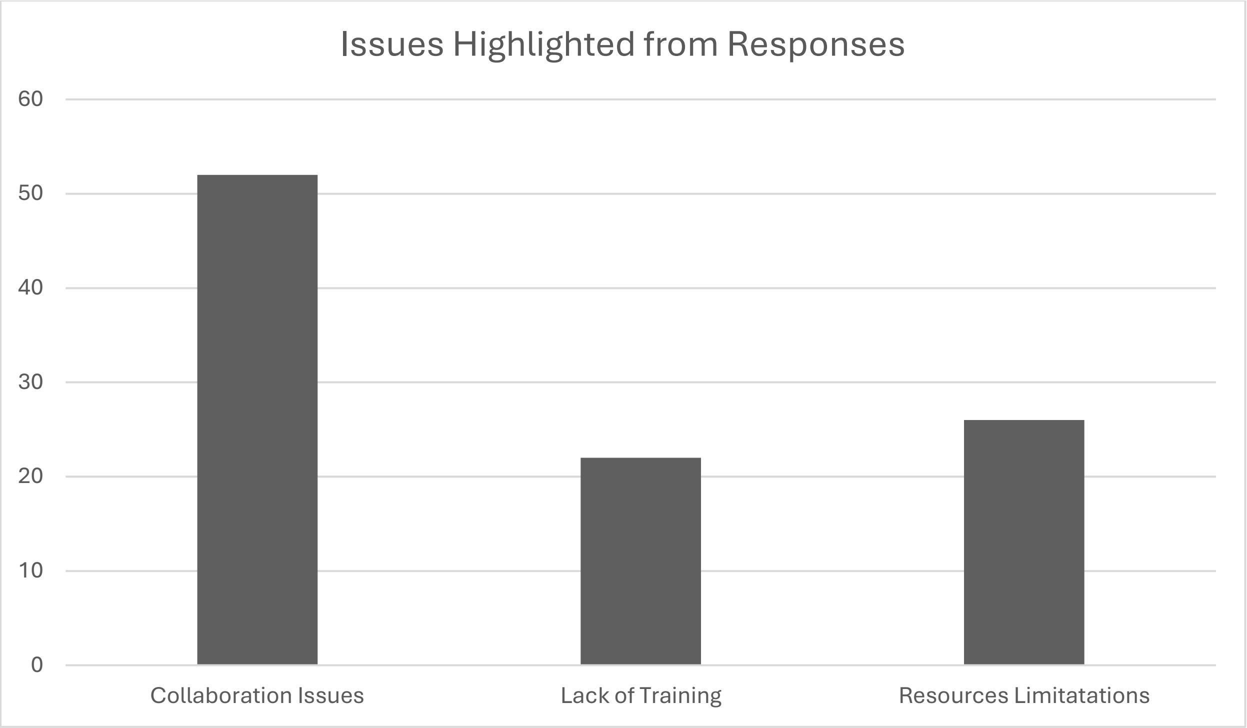


Figure 5.

4.5.3 User Perceptions and Experiences

Survey responses highlighted that while the majority of users (78%) considered existing security measures effective, 22% felt these measures were inadequate. Among those who reported challenges, the most common issues included complexity of security protocols (40%), compatibility problems with existing systems (30%), and restrictive security measures impacting device functionality (30%). Open-ended responses also highlighted frustration with the lack of user-friendly interfaces and insufficient communication about security updates and practices.

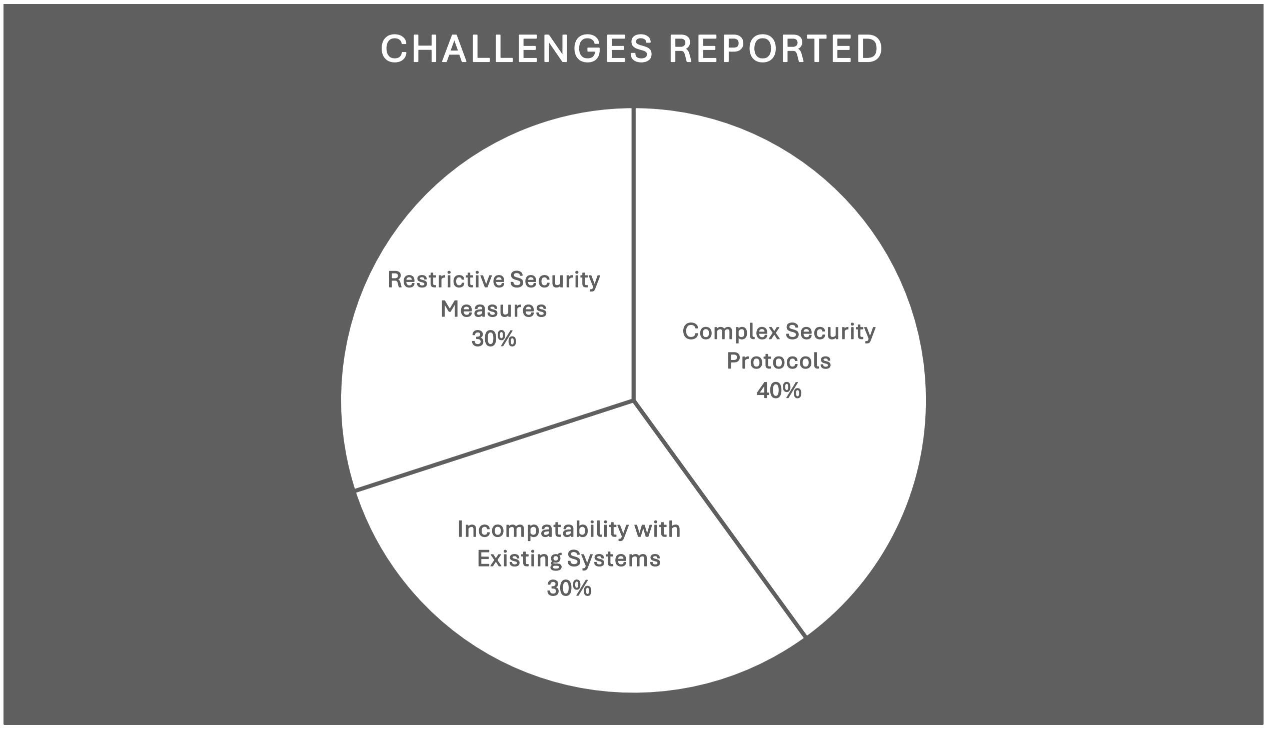


Figure 6.

4.5.4 Vulnerability Findings

The vulnerability assessments revealed that critical security weaknesses were concentrated in specific IoT device categories. 34% of high-risk vulnerabilities were found in surveillance cameras, mostly as a result of out-of-date firmware that left them open to exploitation. 26% of the issues were related to access control systems, and weak default passwords were a common concern that raised the possibility of unwanted access. Due to irregular monitoring and delayed upgrades, devices functioning in heavily trafficked or frequently used contexts, including fleet management systems, displayed 20% of the vulnerabilities, further emphasizing the need for proactive security measures. 15% of vulnerabilities were caused by network monitoring devices, mostly as a result of open ports and setup errors that increased the attack surface. Furthermore, breakdowns and downtimes affecting surveillance cameras and access controls that impair security operations accounted for 5% of the vulnerabilities found.

4.6 Challenges, Risks and Opportunities

4.6.1 Challenges

Managing diverse IoT devices across multiple departments poses significant challenges, as inconsistencies in configurations, updates, and security practices often emerge. Limited technical expertise among staff further hinders effective deployment and maintenance of security measures, leaving devices vulnerable to exploitation. Integration difficulties also arise when IoT devices are not seamlessly compatible with existing IT infrastructure and security systems. Additionally, scalability becomes an issue as the organization increases its use of IoT devices, straining resources and creating gaps in security coverage. Compounding these challenges is the low level of user awareness and training on IoT security protocols, leading to non-compliance and greater risk exposure.

4.6.2 Risks

IoT devices introduce several risks that can have serious repercussions for the organization. One of the most pressing concerns is the potential for data breaches, where compromised devices could expose sensitive organizational or customer information. Device vulnerabilities, such as outdated firmware or misconfigurations, can also lead to compromises where IoT devices are exploited for malicious purposes like botnets or espionage. Operational downtime is another risk, with environmental factors or targeted attacks disrupting critical systems, such as surveillance or access control, leading to inefficiencies. These incidents often result in financial losses, including high recovery costs, legal penalties, and reputational damage. Furthermore, failing to comply with industry standards or regulatory requirements for IoT security could result in audits, fines, or loss of certifications, further impacting the organization.

4.6.3 Opportunities

Despite the challenges and risks, IoT devices present significant opportunities for growth and improvement. Enhanced IoT security can ensure device reliability, improving operational efficiency and reducing downtime. Investing in advanced security technologies, such as AI-driven threat detection and blockchain for secure data transmission, provides the organization with a competitive edge. Implementing centralized device management systems offers better oversight and control of IoT devices, leading to stronger security and optimized performance. Additionally, conducting IoT security awareness programs for employees can foster a culture of security, empowering staff to identify and mitigate risks effectively. Procuring weather-resilient devices with robust fault-tolerant systems mitigates the risks posed by environmental factors while enabling expanded outdoor IoT applications, further strengthening the organization’s IoT ecosystem.

4.7 Conclusion

The cybersecurity environment of IoT devices at Nyaradzo Group Headquarters has been well understood thanks to the analysis of data gathered using a variety of techniques. Significant policy gaps, inconsistent security procedures, and vulnerabilities threatening device integrity and operational effectiveness were found in the findings. A key concern identified was the lack of specific security guidelines for IoT devices, leading to misconfigurations, outdated firmware, and procurement inconsistencies. Limited user awareness and difficulties in collaborating between the IT and security teams were other factors that led to security flaws.

Vulnerability assessments found high-risk exposures in network monitoring devices, access control systems, and surveillance cameras, while survey responses emphasized frustration with intricate security measures. Further contributing to device failures and downtimes were environmental conditions and physical security breaches, underscoring the need for more robust solutions

Despite these challenges, there are opportunities to improve security by implementing innovative security technology, centralizing device management, and improving policies. Increasing staff awareness and training can help to strengthen cybersecurity resilience even further. The insights gained from this analysis serve as a foundation for formulating strategic recommendations to enhance the security and efficiency of IoT devices within the organization.

Chapter 5: SUMMARY, CONCLUSION & RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary, discussion, conclusions, implications, recommendations, and suggestions for further research. The study aimed to assess the cybersecurity measures for IoT devices at Nyaradzo Group Headquarters, identify challenges in integrating cybersecurity solutions, and explore best practices to enhance IoT security. The findings were analysed in relation to the research objectives, leading to key conclusions and actionable recommendations.

5.2 Discussion

This study set out to evaluate the cybersecurity landscape for IoT devices at Nyaradzo Group Headquarters, focusing on existing security measures, integration challenges, and best practices for enhancing cybersecurity. The findings presented provided key insights related to these objectives. The Research Objectives as written in Chapter 1:

1. To evaluate the current cybersecurity measures in place for IoT devices at Nyaradzo Group Headquarters.
2. To identify challenges associated with integrating cybersecurity solutions for IoT devices at Nyaradzo Group.
3. To explore best practices and recommendations for optimizing cybersecurity measures to enhance IoT device security

5.2.1 Addressing Research Objective 1: Evaluating Current Cybersecurity Measures

The first objective aimed to assess the current cybersecurity measures in place for IoT devices at Nyaradzo Group Headquarters. Chapter 4 revealed that while certain security practices exist, there are critical gaps that expose IoT devices to potential risks. The findings highlighted:

- Lack of Standardized Security Policies: IoT security policies were either missing or inconsistently enforced across departments, leading to fragmented security controls.
- Outdated Firmware and Software: Some IoT devices, particularly surveillance cameras and vehicle trackers, had outdated firmware, making them vulnerable to exploitation.
- Inconsistent Security Monitoring: The absence of real-time monitoring and centralized threat detection systems resulted in delayed responses to security incidents.
- Procurement of Insecure Devices: Inconsistent procurement processes led to the acquisition of IoT devices with inadequate security features, such as a lack of encryption and tamper detection.
- Environmental Vulnerabilities: Outdoor IoT devices, such as motion sensors and surveillance cameras, were affected by environmental factors, leading to system failures and false alarms.

These findings indicate that while Nyaradzo Group has implemented some security measures, significant vulnerabilities remain, necessitating a more structured and comprehensive approach to IoT cybersecurity.

5.2.2 Addressing Research Objective 2: Identifying Challenges in Integrating Cybersecurity Solutions

The second objective focused on the challenges associated with implementing IoT cybersecurity solutions at Nyaradzo Group. The findings in Chapter 4 identified several key challenges:

- Inconsistent procurement policies, leading to the acquisition of IoT devices with varying security standards.
- Integration difficulties between IoT security systems and the existing IT infrastructure, causing compatibility issues.
- Limited expertise and awareness among employees, increasing the risk of security breaches due to human error.
- Insufficient budget allocation for cybersecurity enhancements, restricting the implementation of advanced security solutions.

These challenges indicate the need for a more structured approach to IoT security, including better procurement policies, improved system integration strategies, and enhanced cybersecurity training for employees.

5.2.3 Addressing Research Objective 3: Exploring Best Practices for Optimizing IoT Cybersecurity

The third objective sought to identify best practices and recommendations for improving IoT cybersecurity. Based on the findings discovered, the study identified several strategies that could enhance security:

- Implementing Multi-Factor Authentication (MFA) to strengthen user access control.
- Adopting AI-driven security solutions for real-time threat detection and response.
- Establishing a centralized IoT management framework to ensure all devices follow a uniform security policy.
- Conducting continuous employee training to improve cybersecurity awareness and reduce human-related vulnerabilities.
- Enhancing regulatory compliance by aligning security policies with industry standards.

By implementing these best practices, Nyaradzo Group can significantly enhance its IoT security framework and reduce the risk of cyber threats.

5.3 Conclusion

The study concluded that while Nyaradzo Group has established fundamental cybersecurity measures for IoT devices, there are notable gaps in policy enforcement, real-time monitoring, and standardization across devices. The integration of cybersecurity solutions remains a challenge due to inconsistent procurement policies, technical incompatibilities, and limited cybersecurity expertise among employees. Addressing these issues requires a multi-faceted approach that includes strategic investment in cybersecurity infrastructure, enhanced employee training, and adherence to global security standards. The research also underscored the importance of adopting AI-driven threat detection, centralized security management frameworks, and continuous policy improvements to enhance IoT security resilience.

5.4 Implications

5.4.1 Practical Implications

- For IT Management: The study highlights the need for more robust IoT security policies and improved enforcement of cybersecurity best practices.

- For Employees: Greater cybersecurity awareness and training are necessary to reduce human-related security risks.

- For Procurement Teams: Strengthening procurement policies can ensure only secure IoT devices are acquired and deployed.

5.4.2 Theoretical Implications

This study contributes to the body of knowledge on IoT cybersecurity, particularly in organizational contexts, by providing insights into the challenges, risks, and best practices for securing IoT devices. It highlights the importance of implementing robust security measures to mitigate cyber threats and ensure the reliability of IoT systems within an enterprise setting. Furthermore, the study aligns with the Technology Acceptance Model (TAM) by emphasizing how the perceived ease of use and usefulness of cybersecurity measures influence their adoption within an organization. Additionally, it incorporates the Resource-Based View (RBV) by demonstrating how strong cybersecurity policies and technologies serve as strategic assets that enhance operational efficiency and provide a competitive advantage. By securing IoT devices effectively, organizations can minimize security risks, improve productivity, and maintain trust in their digital infrastructure.

5.4.3 Policy Implications

The study suggests that organizations should align their IoT security policies with global frameworks such as NIST (National Institute of Standards and Technology) and ISO/IEC 27001, which provide standardized guidelines for managing cybersecurity risks effectively. Adhering to these frameworks can help organizations establish structured security protocols, improve risk assessment processes, and enhance overall resilience against cyber threats. Additionally, the study emphasizes the need for developing cybersecurity governance structures that clearly define roles and responsibilities for IoT security management. By assigning dedicated personnel or teams to oversee IoT security, organizations can ensure consistent policy enforcement, streamline incident response efforts, and maintain accountability in safeguarding their digital assets. Implementing these measures will strengthen IoT security frameworks, ultimately reducing vulnerabilities and improving the organization's overall cybersecurity posture.

5.5 Recommendations

To mitigate cybersecurity risks and enhance IoT security at Nyaradzo Group, the following recommendations are proposed:

5.5.1 Strengthening Security Policies

Organizations should develop and enforce comprehensive IoT security policies that cover key aspects such as procurement, configuration, and maintenance standards. A well-defined policy framework ensures that all IoT devices acquired meet minimum security requirements, including encryption, firmware update capabilities, and tamper detection. Proper configuration guidelines will help mitigate vulnerabilities associated with default settings, weak passwords, and open network ports, while maintenance standards will ensure that devices receive regular updates and security patches to address emerging threats.

Additionally, it is crucial to establish clear accountability structures to ensure security compliance across all departments. Assigning specific roles and responsibilities for IoT security management will enhance coordination between IT, cybersecurity, and operational teams, reducing inconsistencies in security practices. This approach will also streamline incident response efforts, ensuring that security breaches are promptly identified and mitigated. By integrating these measures, organizations can strengthen their IoT security posture, minimize risks, and maintain a secure and resilient digital infrastructure.

5.5.2 Enhancing Security Controls

To enhance IoT security, organizations should implement multi-factor authentication (MFA) to strengthen access controls and prevent unauthorized use of critical systems. MFA adds an extra layer of security by requiring multiple verification factors, such as passwords, biometric authentication, or one-time passcodes, reducing the risk of unauthorized access even if credentials are compromised.

Additionally, enforcing data encryption and regular patch management is essential to minimize vulnerabilities in IoT devices. Encryption ensures that data transmitted between devices and networks remains secure from interception or tampering, while regular patching helps address known security flaws, reducing the likelihood of exploitation by cyber attackers.

To further improve security, organizations should deploy AI-driven monitoring systems capable of detecting and responding to security threats in real time. AI-based security solutions can analyze network traffic patterns, identify anomalies, and automatically respond to potential cyber threats before they escalate. This proactive approach enhances the organization's ability to mitigate risks, reduce downtime, and maintain the integrity of its IoT ecosystem.

5.5.3 Improving Cybersecurity Awareness

Organizations should conduct regular cybersecurity training for employees to enhance their understanding of potential threats and best security practices. Training sessions should cover topics such as identifying phishing attempts, securing IoT devices, using strong authentication methods, and responding to security incidents. By ensuring that employees are well-informed about cybersecurity risks, organizations can significantly reduce vulnerabilities caused by human error.

In addition to formal training, companies should develop an internal cybersecurity awareness program to promote a culture of security best practices. This program can include regular security updates, simulated phishing exercises, awareness campaigns, and easy-to-follow security guidelines tailored to IoT security. By fostering continuous learning and engagement, organizations can improve compliance with security policies, minimize cyber risks, and strengthen their overall cybersecurity posture.

5.5.4 Strengthening Procurement and Infrastructure

Organizations should standardize procurement procedures to ensure that only secure IoT devices are acquired. This involves establishing strict security criteria for IoT devices before purchase, including encryption capabilities, firmware update mechanisms, and tamper detection features. A standardized procurement process will help eliminate inconsistencies in security measures across different departments, reducing the risk of integrating vulnerable devices into the organization's network.

Additionally, it is crucial to ensure that all IoT devices have security certifications before deployment. Certifications such as ISO/IEC 27001, NIST cybersecurity compliance, or manufacturer-specific security standards provide assurance that the devices meet industry-recognized security benchmarks. By enforcing these standards, organizations can minimize security risks, enhance compliance with regulatory requirements, and maintain a more secure and resilient IoT ecosystem.

5.6 Suggestions for Further Research

While this study provided valuable insights into the cybersecurity challenges and solutions for IoT devices at Nyaradzo Group, further research is necessary to deepen the understanding of emerging security threats and best practices. Future studies could explore the following areas:

1. Effectiveness of AI and Machine Learning in IoT Cybersecurity: Future research could examine how artificial intelligence and machine learning can be leveraged to enhance real-time threat detection, anomaly detection, and predictive security models for IoT devices in corporate environments.

2. Comparative Analysis of IoT Security Frameworks Across Different Industries: Conducting a study that compares the cybersecurity practices of different industries that heavily rely on IoT devices (e.g., healthcare, finance, and logistics) could provide insights into best practices that could be adapted for the funeral services sector.

3. Incident Response and Recovery Strategies for IoT Security Breaches: Examining best practices for handling IoT-related security breaches, including response times, mitigation strategies, and business continuity planning in organizations relying on IoT infrastructure.

By addressing these areas, future research can contribute to the ongoing efforts to enhance IoT security in the funeral services sector and beyond.

References

- Barney, J. B. (1991). The resource-based view of the firm: Capabilities, strategic assets and the course of competition. Strategic Management Journal, 12(S1), 649-668.
- Clarke, R. (2009). Privacy impact assessment. International Data Privacy Law, 1(1), 1-17.
- DeLone, W. H., & McLean, E. R. (1992). Information systems success model: The IS success model: A theoretical framework and an empirical investigation. Journal of Management Information Systems, 9(1), 9-30.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.
- National Institute of Standards and Technology (NIST). (2011). Risk Management Framework (RMF) for Information Systems and Organizations: Special Publication 800-37. National Institute of Standards and Technology.
- Davis, F. D. (1989). (Chapter 1 reference for Technology Acceptance Model (TAM))
- DeLone, W. H., & McLean, E. R. (1992). (Chapter 1 reference for Information Systems Success Model)
- Barney, J. B. (1991). (Chapter 1 reference for Resource-Based View (RBV))
- Clarke, R. (2009). (Chapter 1 reference for Privacy Impact Assessment (PIA))
- National Institute of Standards and Technology (NIST). (2011). (Chapter 1 reference for Risk Management Framework (RMF))
- Clarke, R. (2009). Privacy impact assessment. International Data Privacy Law, 1(1), 1-17.

- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787-2805.
- Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. Computer Communications, 54, 1-31.
- Gartner, Inc. (2021). Best practices for securing IoT devices in enterprise environments. Gartner Research.
- IoT Security Foundation (2020). IoT security compliance framework. IoT Security Foundation Report.
- Mukherjee, M., Matam, R., Shu, L., Maglaras, L., Ferrag, M. A., Choudhury, N., & Kumar, V. (2017). Security and privacy in fog computing: Challenges, issues, and future directions. IEEE Access, 5, 19293-19304.
- National Institute of Standards and Technology (NIST). (2020). Considerations for managing Internet of Things (IoT) cybersecurity and privacy risks: Special Publication 800-183. National Institute of Standards and Technology.
- Schneier, B. (2019). Click here to kill everybody: Security and survival in a hyper-connected world. W.W. Norton & Company.
- Stouffer, K., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to industrial control systems (ICS) security. NIST Special Publication 800-82 Rev. 2.
- Weber, R. H. (2010). Internet of Things—New security and privacy challenges. Computer Law & Security Review, 26(1), 23-30.

Appendices

Informed Consent

My name is Munyaradzi D. Nkhoma, and I am a final year Computer Information Systems student at Africa University. I am conducting a study to examine: The impact of adopting and implementing cyber security measures to protect the IoT Devices at Nyaradzo Group Headquarters. You have been chosen to participate in this study due to your role as a stakeholder at Nyaradzo.

If you agree to participate, you will be asked to complete a questionnaire or take part in a brief interview, which will take approximately 10-20 minutes of your time. There is no anticipated harm or risk involved in this study, and its purpose is to provide Nyaradzo Group with insights to cybersecurity measures protecting the IoT devices on-premise environments. Your personal details will remain confidential and will not be disclosed without your explicit consent, except if required by law.

Participation in this study is entirely voluntary. Declining to participate will not affect your relationship with Nyaradzo Group or any other party. If you choose to participate, you are free to withdraw your consent and discontinue your participation at any time without any penalty.

Before signing this form, please ask any questions you may have about the study. Take all the time you need to consider your decision. By signing below, you confirm that you have read and understood the information provided in this consent form. You voluntarily agree to participate in this research study and acknowledge your right to withdraw at any time.

--- -----------------------------

Name of Research Participant (please print) Date

Signature of Research Participant or legally authorised representative

If you have any questions concerning this study or consent form beyond those answered by the researcher including questions about the research, your rights as a research participant, or if you feel that you have been treated unfairly and would like to talk to someone other than the researcher, please feel free to contact the Africa University Research Ethics Committee on telephone (020) 60075 or 60026 extension 1156 email aurec@africau.edu

Interview Questions

1. What IoT devices are currently in use at Nyaradzo Group Headquarters?
2. Can you describe the cybersecurity measures currently implemented for these devices?
3. How often are these cybersecurity measures reviewed and updated?
4. Are there any specific cybersecurity policies or procedures in place for IoT devices?
5. What challenges have you encountered in integrating cybersecurity solutions for IoT devices?
6. How do you prioritize cybersecurity investments for IoT devices compared to other IT systems?
7. What are the main obstacles to adopting advanced cybersecurity technologies for IoT devices?
8. What is the level of collaboration between IT and security departments regarding IoT security?
9. How do you stay updated on emerging IoT security threats and vulnerabilities?
10. What are the key factors to consider when selecting cybersecurity solutions for IoT devices?
11. How do you measure the effectiveness of your IoT security measures?
12. What are your expectations for the future of IoT security?

Questionnaire

Section A: Respondent Information

1. **Department:** (e.g., IT, Finance, Claims, Premiums etc.)
2. Job Title:
3. Do you have regular interaction with IoT devices in your role?
    - Yes
    - No

Section B: Perception of Cybersecurity Measures

1. Are you aware of the cybersecurity measures implemented to protect IoT devices at Nyaradzo Group?
    - Yes
    - No
2. In your opinion, how effective are the current cybersecurity measures in protecting IoT devices from cyber threats?
    - Not effective
    - Somewhat effective
    - Effective
    - Very effective
3. Have you encountered any difficulties due to the implementation of cybersecurity measures for IoT devices? (e.g., complexity, compatibility issues)

- Yes
- No

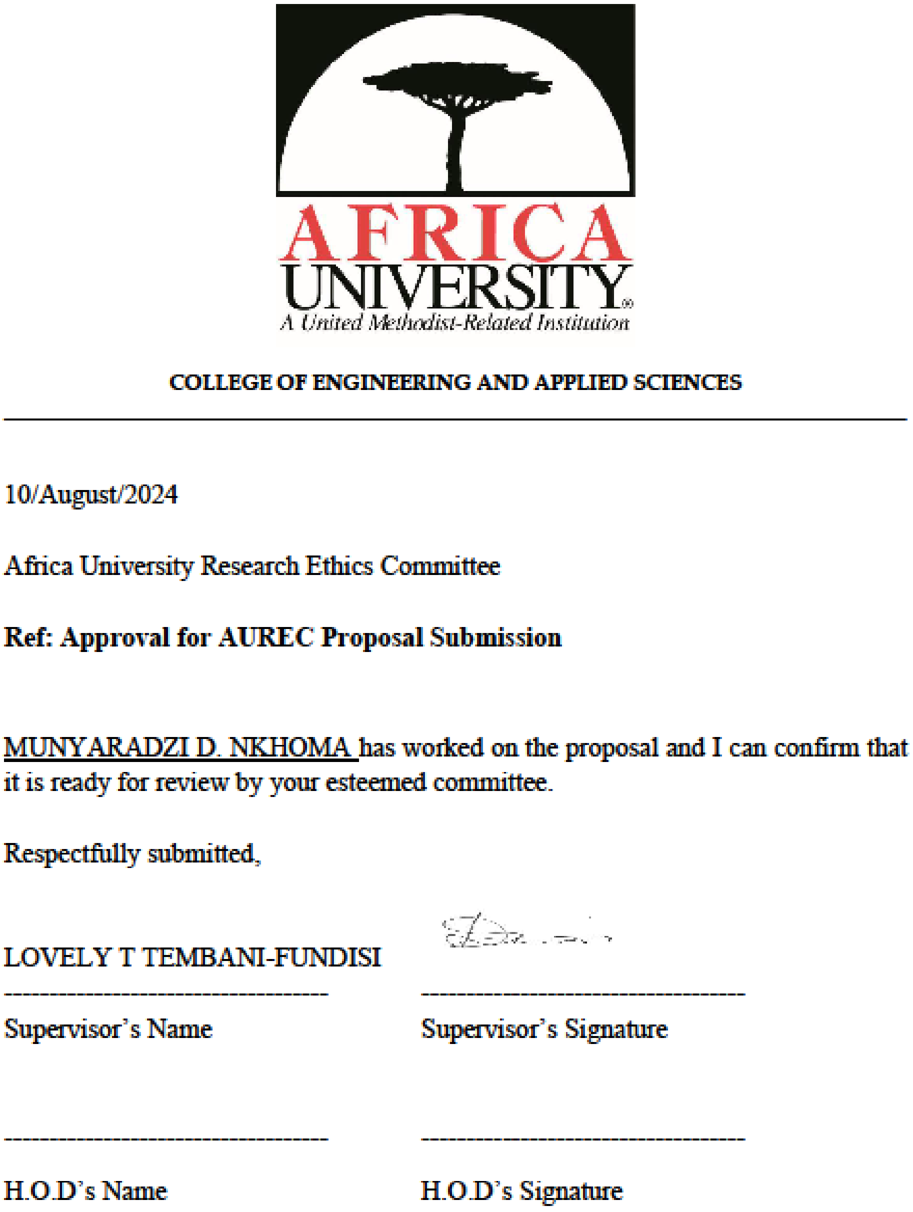
4. If yes, please elaborate on the difficulties you have encountered. (Open-ended)

Section D: Additional Comments

Please provide any additional comments or suggestions you may have regarding cybersecurity measures for IoT devices at Nyaradzo Group Headquarters. (Open-ended)

Thank you for your time and participation!

Supervisor's Approval



AFRICA UNIVERSITY®
A United Methodist-Related Institution

COLLEGE OF ENGINEERING AND APPLIED SCIENCES

10/August/2024

Africa University Research Ethics Committee

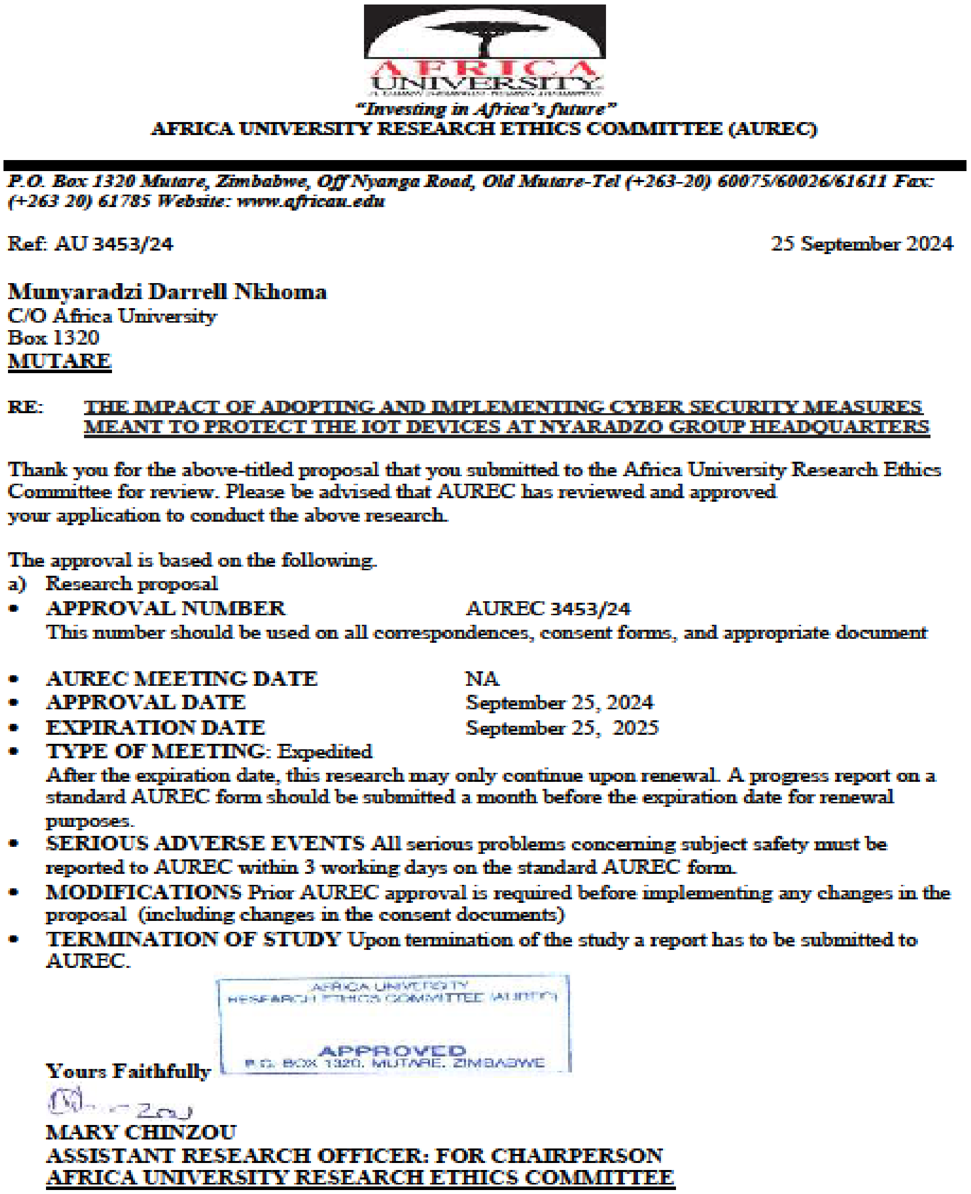
Ref: Approval for AUREC Proposal Submission

MUNYARADZI D. NKHOMA has worked on the proposal and I can confirm that it is ready for review by your esteemed committee.

Respectfully submitted,

LOVELY T TEMBANI-FUNDISI	
------------------------------------	------------------------------------
Supervisor's Name	Supervisor's Signature
------------------------------------	------------------------------------
H.O.D's Name	H.O.D's Signature

AUREC Approval



AFRICA UNIVERSITY

"Investing in Africa's future"

AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE (AUREC)

P.O. Box 1320 Mutare, Zimbabwe, Off Nyanga Road, Old Mutare-Tel (+263-20) 60075/60026/61611 Fax: (+263 20) 61785 Website: www.africau.edu

Ref: AU 3453/24 — 25 September 2024

Munyaradzi Darrell Nkhoma
C/O Africa University
Box 1320
MUTARE

RE: THE IMPACT OF ADOPTING AND IMPLEMENTING CYBER SECURITY MEASURES MEANT TO PROTECT THE IOT DEVICES AT NYARADZO GROUP HEADQUARTERS

Thank you for the above-titled proposal that you submitted to the Africa University Research Ethics Committee for review. Please be advised that AUREC has reviewed and approved your application to conduct the above research.

The approval is based on the following.
a) Research proposal

- **APPROVAL NUMBER** AUREC 3453/24
  This number should be used on all correspondences, consent forms, and appropriate document

- **AUREC MEETING DATE** NA
- **APPROVAL DATE** September 25, 2024
- **EXPIRATION DATE** September 25, 2025
- **TYPE OF MEETING:** Expedited
  After the expiration date, this research may only continue upon renewal. A progress report on a standard AUREC form should be submitted a month before the expiration date for renewal purposes.
- **SERIOUS ADVERSE EVENTS** All serious problems concerning subject safety must be reported to AUREC within 3 working days on the standard AUREC form.
- **MODIFICATIONS** Prior AUREC approval is required before implementing any changes in the proposal (including changes in the consent documents)
- **TERMINATION OF STUDY** Upon termination of the study a report has to be submitted to AUREC.

AFRICA UNIVERSITY
RESEARCH ETHICS COMMITTEE (AUREC)
APPROVED
P.O. BOX 1320, MUTARE, ZIMBABWE

Yours Faithfully

MARY CHINZOU
ASSISTANT RESEARCH OFFICER: FOR CHAIRPERSON
AFRICA UNIVERSITY RESEARCH ETHICS COMMITTEE