UNIVERSITY OF CAPE COAST

THE IMPACT OF CYBERSECURITY ON HEALTH SECTORS BEFORE AND AFTER COVID-19

BENNISON MARTINSON ASOMAH

AMOA-MENYAH EMMANUEL

DOMEH JOHN KINGSMAN AFRIYIE

2023

Bennison Martinson Asomah

Amoa-Menyah Emmanuel

Domeh John Kingsman Afriyie

University of Cape Coast

UNIVERSITY OF CAPE COAST

THE IMPACT OF CYBERSECURITY ON HEALTH SECTORS BEFORE AND AFTER COVID-19

BY.

PS/CSC/19/0123; BENNISON MARTINSON ASOMAH

PS/CSC/19/0093; AMOA-MENYAH EMMANUEL

PS/CSC/19/0103; DOMEH JOHN KINGSMAN AFRIYIE

SUPERVISED BY; **MR. PAUL K. ARHIN JNR**

A project submitted to the Department of Computer Science and Information Technology of the College of Agriculture and Natural Science, University of Cape Coast, in partial fulfillment of the requirement for the award of Bachelor of Science degree in Computer Science.

SEPTEMBER,2023

DECLARATION

Candidate's Declaration

I hereby declare that this project work is the result of my own original research and that no part of it has been presented for another degree in this university or elsewhere.

Candidate's Signature: ..... Date: .....

Name: Asomah Bennison Martinson

Candidate's Signature: ..... Date: .....

Name: Amoa-Menyah Emmanuel

Candidate's Signature: ..... Date: .....

Name: Domeh John Kingsman Afriyie

Supervisor's Declaration

I hereby declare that the preparation and presentation of the project work were supervised in accordance with the guidelines on supervision of thesis laid down by the University of Cape Coast.

Supervisor's Signature: ..... Date: .....…

Name: Mr. Paul K. Arhin Jnr

ABSTRACT

This study examines the evolving landscape of hospital cybersecurity in the wake of the COVID-19 pandemic. Through a mixed-methods approach including literature synthesis, quantitative and qualitative analysis, the research investigates perspectives, challenges, and mitigation strategies within hospital IT departments and administrations.

Purpose: This research aims to understand the impact of COVID-19 on hospital cybersecurity, exploring vulnerabilities, threats, and measures adopted before and after the pandemic.

Methodology: The study employed online questionnaires to collect data from IT departments and administrations in five hospitals. The data was analyzed quantitatively and qualitatively, with cross-analysis to compare responses.

Findings: Literature synthesis highlights vulnerabilities stemming from rapid digitization during the pandemic, underscoring the need for proactive cybersecurity measures. Demographics reveal gender, age, roles, and hospital affiliations of respondents. Quantitative analysis within IT departments outlines security tools, risk perception, audit frequency, disaster recovery plans, and phishing experiences. Qualitative insights reveal challenges and strategies, while administration perspectives focus on impact and mitigation strategies.

Conclusion: This study provides valuable insights into the intricate landscape of hospital cybersecurity in the context of the COVID-19 pandemic.

ACKNOWLEDGEMENTS

Our gratitude extends to Mr. Paul Arhin, our guide, Attrams Papa Odame, the supportive IT department and administrators, and our friends. We also acknowledge the invaluable assistance of a natural language processing tool in our research compilation.

DEDICATION

This work is dedicated to our department, our family and dear friends.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Table Pages

LIST OF FIGURES

Figure Page

LIST OF ABBREVIATIONS

EHRs	Electronic Health Records
IoMT	Internet of Medical Things
AI	Artificial Intelligence
ML	Machine Learning
UHS	Universal Health Services

CHAPTER ONE

INTRODUCTION

Background to the Study

The COVID-19 pandemic has ushered in a new era of challenges and transformations for the global healthcare sector. With healthcare systems grappling to adapt to the demands of the pandemic, the rapid shift towards digitization and remote healthcare solutions has introduced unprecedented opportunities and vulnerabilities. As hospitals strive to balance patient care, operational efficiency, and data security, the intersection of healthcare and cybersecurity has become a critical concern. (Filip et al., 2022)

Statement of the Problem

The convergence of the COVID-19 pandemic and the digitization of healthcare services has brought forth an array of cybersecurity threats to hospitals. As healthcare organizations hastily embraced digital solutions, they have become targets for malicious actors seeking to exploit vulnerabilities in critical medical infrastructure, patient data, and operations. The pressing need to understand the impact of these threats on hospitals and healthcare delivery has given rise to the research problem explored in this study. (He et al., 2020)

Purpose of the Study

The purpose of this study is to examine the impact of cybersecurity challenges on healthcare organizations, particularly hospitals, before and after the COVID-19 pandemic. By investigating the evolving cybersecurity landscape in healthcare, this research aims to uncover the vulnerabilities, threats, and mitigation strategies that have emerged due to the pandemic-induced digital transformation. The study seeks to provide valuable insights into safeguarding the integrity of healthcare systems and patient data in the face of mounting cyber risks.

Research Questions

This research addresses the following key research questions:

1. What are the significant cybersecurity threats that healthcare organizations, especially hospitals, have faced before and after the COVID-19 pandemic?

2. How have these cybersecurity threats evolved and manifested because of the digitalization of healthcare services during the pandemic?

3. What measures and strategies can healthcare organizations adopt to mitigate the impact of cybersecurity threats and enhance the security of patient data and critical medical infrastructure?

Significance of the Study

The findings of this study hold profound implications for the healthcare sector, hospital administrators, IT professionals, policymakers, and researchers. By shedding light on the cybersecurity vulnerabilities exposed by the pandemic, this research can guide healthcare organizations in proactively bolstering their cyber defenses. Furthermore, the study contributes to the broader understanding of the complex interplay between healthcare, technology, and security in times of crisis.

Limitations of the Study

While this study strives to provide comprehensive insights into the impact of cybersecurity threats on healthcare organizations, there are certain limitations. The study's scope is focused on hospitals and may not encompass all aspects of the healthcare ecosystem. Additionally, the reliance on self-reported data from online questionnaires introduces potential biases and limitations in the data collection process.

Organization of the Study

The remainder of this research is organized as follows:

Chapter 2 - Literature Review: This chapter offers a synthesis of pertinent literature to establish the existing knowledge and identify gaps regarding the impact of COVID-19 on hospital cybersecurity. It delves into studies, reports, and scholarly works that shed light on the evolving cybersecurity landscape within healthcare.

Chapter 3 - Methodology: In this chapter, the research methodology is delineated, encompassing data collection methods, participant selection, and the tools employed. The chapter outlines the systematic approach employed to gather and analyze data from healthcare professionals.

Chapter 4 - Results and Discussion: This chapter presents the outcomes derived from the data analysis, offering a comprehensive depiction of the perspectives, challenges, and mitigation strategies related to hospital cybersecurity. The findings are presented in a structured manner to illuminate key insights. Following the presentation of results, the research results in light of the existing literature, providing a contextual analysis of the implications of the study's findings. It explores the broader implications of the results and examines how they align with or deviate from prior research.

Chapter 6 - Summary and Conclusion: The final chapter encapsulates the study's journey, summarizing the key findings, insights, and implications. It also outlines the conclusions drawn from the research and offers recommendations for healthcare organizations to bolster their cybersecurity strategies.

Throughout the study, efforts are made to synthesize the findings, present their implications, and contribute to the broader understanding of cybersecurity challenges in the healthcare sector.

CHAPTER TWO

LITERATURE REVIEW

Relevance of Literature to Objectives/Research Questions

The COVID-19 outbreak has presented an array of challenges to global healthcare services. The heightened reliance on Information Technology (IT) systems and rapid digitization during the pandemic has exposed hospitals to substantial cybersecurity threats. This review aims to explore the repercussions of COVID-19 on hospital cybersecurity, focusing on vulnerabilities, threats, key findings, recommendations, mitigation strategies, and the safeguarding of critical healthcare infrastructure. (Filip et al., 2022)

Demonstration of Scholarly Analysis and Criticism

This chapter conducts an in-depth scholarly analysis and critique of pertinent research aligned with the study's objectives. By critically evaluating methodologies, outcomes, and limitations of prior studies, this analysis reinforces the urgency of comprehending the evolving interplay between COVID-19-driven healthcare transformation and escalating cybersecurity risks.

Digitalization Trends in Healthcare

Within the realm of healthcare, digitalization trends have witnessed notable acceleration in recent years. These trends leverage technology and data to enhance patient care, operational efficiency, and innovative practices.

Telemedicine and Virtual Care: Telemedicine's growth, particularly amid the pandemic, has revolutionized remote healthcare delivery, allowing video consultations, diagnosis, and treatment. It enhances access to healthcare, particularly in remote areas, while reducing the need for in-person visits. (Kichloo et al., 2020)

Electronic Health Records (EHRs): EHRs have supplanted paper-based medical records, enabling secure, centralized storage of patient data. Real-time access to patient information, streamlined documentation, care coordination, and data-driven decisions are facilitated. (HealthIT.gov, 2022)

Internet of Medical Things (IoMT): IoMT integrates medical devices, wearables, and sensors with healthcare systems, enabling real-time data collection, remote patient monitoring, and personalized care. IoMT spans applications such as wearable fitness trackers and implantable devices. (Srivastava et al., 2022)

Artificial Intelligence (AI) and Machine Learning (ML): AI and ML technologies are leveraged for clinical decision-making, personalized treatment planning, and administrative task automation. Their transformative impact on healthcare efficiency and error reduction is evident. (Javaid et al., 2022)

Blockchain in Healthcare: Blockchain's secure and decentralized nature holds promise for healthcare data management, interoperability, and privacy. It can elevate patient data security, streamline medical records sharing, and optimize clinical trials and supply chain management. (Tagde et al., 2021)

Case Study: Universal Health Services (UHS) Cyberattack

The case study of the UHS cyberattack in September 2020 underscores the tangible ramifications of inadequate cybersecurity measures. The ransomware attack on UHS disrupted operations across its facilities, causing extensive system outages and affecting patient care. (Jercich, 2021)

Impact on Healthcare Organizations

Drawing insights from diverse sources, this section examines the tangible impact of cybersecurity incidents on healthcare institutions. It accentuates the potential disruptions to patient care, financial repercussions, reputational damage, and legal consequences, underscoring the gravity of cyber threats and the imperative of proactive cybersecurity strategies. (He et al., 2020)

Conclusion

Chapter 2 concludes by synthesizing lessons drawn from previous research and real-world incidents in healthcare cybersecurity. It encapsulates the essence of research objectives by emphasizing data protection, regular vulnerability assessments, incident response readiness, and effective communication within healthcare systems. The organization of this chapter aligns with research objectives and guides the reader through the progressive evolution of healthcare cybersecurity concerns amidst the pandemic's digital transformation.

Organization of Literature

This chapter's meticulous organization adheres to research objectives, underpinning the logical flow of the study. It transitions from contextualizing the impact of COVID-19 to exploring digitalization trends, showcasing real-world consequences, and highlighting the implications for healthcare organizations. This systematic arrangement enables readers to grasp the intricacies of healthcare cybersecurity's evolution and the imminent challenges it presents.

In sum, Chapter 2 critically examines literature to establish theoretical foundations and logical progression. It underscores the nexus between healthcare digitalization and cybersecurity vulnerabilities, thus paving the way for ensuing chapters that delve into findings, analysis, and recommendations to fortify hospital cybersecurity in the post-pandemic landscape.

CHAPTER THREE

METHODOLOGY

This chapter outlines the methodology employed in the study "The Impact of Cybersecurity on Health Sectors Before and After Covid-19." The methodology is tailored to address the research objectives, encompassing the research design, study area, data collection instruments, reliability and validity, data analysis, ethical considerations, and limitations.

Methodology to Achieve Objectives

To comprehensively investigate the intricate relationship between cybersecurity and the healthcare sector, a mixed-methods research design was strategically chosen. This approach seamlessly integrates quantitative and qualitative methodologies, ensuring a comprehensive exploration of both statistical trends and nuanced insights from healthcare and cybersecurity stakeholders.

Quality and Relevant Data Collection Instruments

The primary instrument for data collection was a structured online questionnaire. This instrument was meticulously divided into three distinct sections:

Demographic Characteristics

Captured essential respondent information.

Security Tools and Attacks

Explored computer security tools, threats, defense mechanisms, and incident response.

Forms of Attacks on Victims

Investigated various attack types, their impact, and mitigation strategies.

Data Collection Instruments

1.Data Collection Instruments

Construct	No. of items	Type
Demographic characteristics	2	Multiple choice
Security tools and attacks	20	Multiple choice, short answers, 5-point Likert scale,
Forms of attacks on victims	10	Multiple choice, short answers, 5-point Likert scale

Construct Source: (Martin & Marsh, 2006)

Each section was thoughtfully designed to ensure a comprehensive and detailed exploration of the research domain. The data collection process integrated various question types, including multiple-choice, check boxes, short answers, and a 5-point Likert scale, ranging from 1 (lowest) to 5 (highest).

Data Collection and Analysis Procedures

Data collection was conducted via Google Forms, allowing seamless administration of the online questionnaire. The sample consisted of respondents from both the administration and IT departments of the hospitals mentioned earlier. The Google Forms platform facilitated streamlined data collection and storage.

Reliability and Validity

Internal consistency was employed to assess the reliability of the constructs. This method evaluates the correlation among multiple items in a test designed to measure the same underlying construct.

Additionally, rigorous pre-testing and consultation with an expert ensured the validity of the data collected.

Ethical Considerations

Research ethics played a pivotal role in this study. Strict ethical guidelines were followed, ensuring participants' confidentiality and anonymity. Informed consent was obtained from all participants before their engagement in the online questionnaire.

Limitations

While extensive efforts were undertaken to ensure the study's robustness, certain limitations were acknowledged. The reliance on online questionnaires may have implications for the depth of insights compared to in-person interviews. Additionally, the rapidly evolving nature of cybersecurity and healthcare practices posed potential challenges during the research period.

In summary, this chapter meticulously aligns with the research's objectives by adopting an appropriate mixed-methods approach, employing quality data collection instruments, and adhering to ethical guidelines. The comprehensive methodology is tailored to provide a holistic understanding of the dynamic interplay between cybersecurity and the healthcare sect

CHAPTER FOUR

RESULTS AND DISCUSSIONS

Overview

This chapter delves into the interpretation and contextualization of the results obtained from the data analysis. It explores the implications of these findings within the broader context of hospital cybersecurity, particularly in the wake of the COVID-19 pandemic.

NB. it should be noted that we used a sample size of 20 out of the larger pool for the purpose of analyzing a represented average of the study population.

RESULTS

Quantitative Analysis

Socio-demographic characteristics

Gender distribution

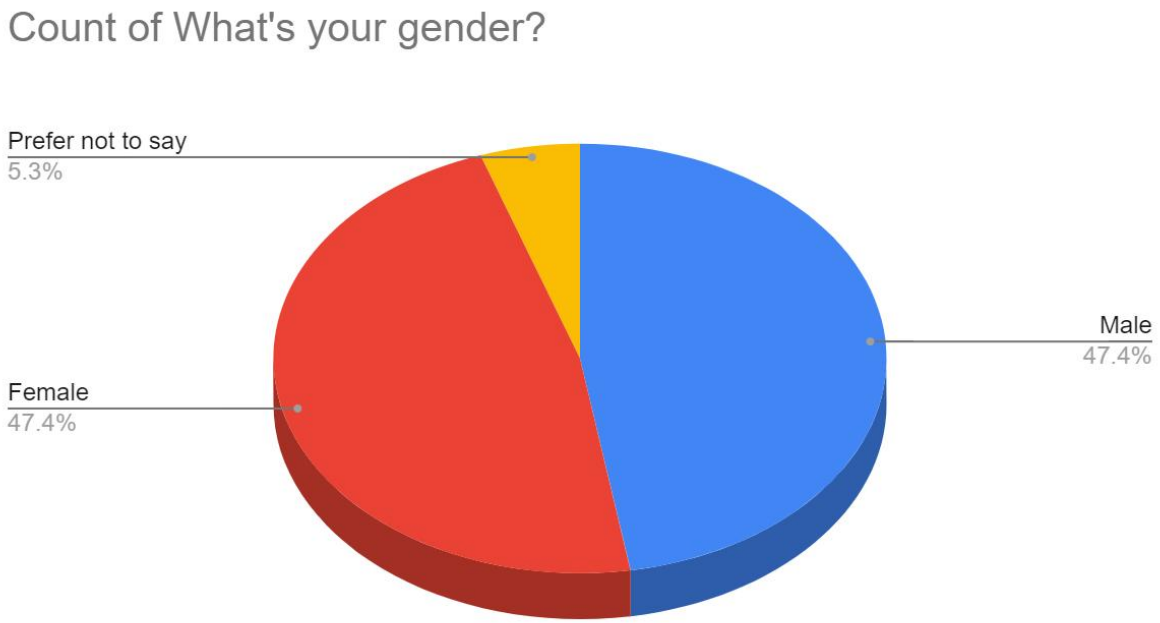

fig4.1

The survey data shows a nearly equal distribution between Male and Female respondents, with Males comprising 50% and Females comprising 45% of the total. This balanced representation suggests that the survey reached a diverse audience and successfully captured a variety of gender identities. The inclusion of the "Prefer not to say" option acknowledges the importance of individual privacy and autonomy. This option allows respondents to decline sharing their gender identity, which is particularly significant when considering the sensitive nature of personal information.

Age distribution

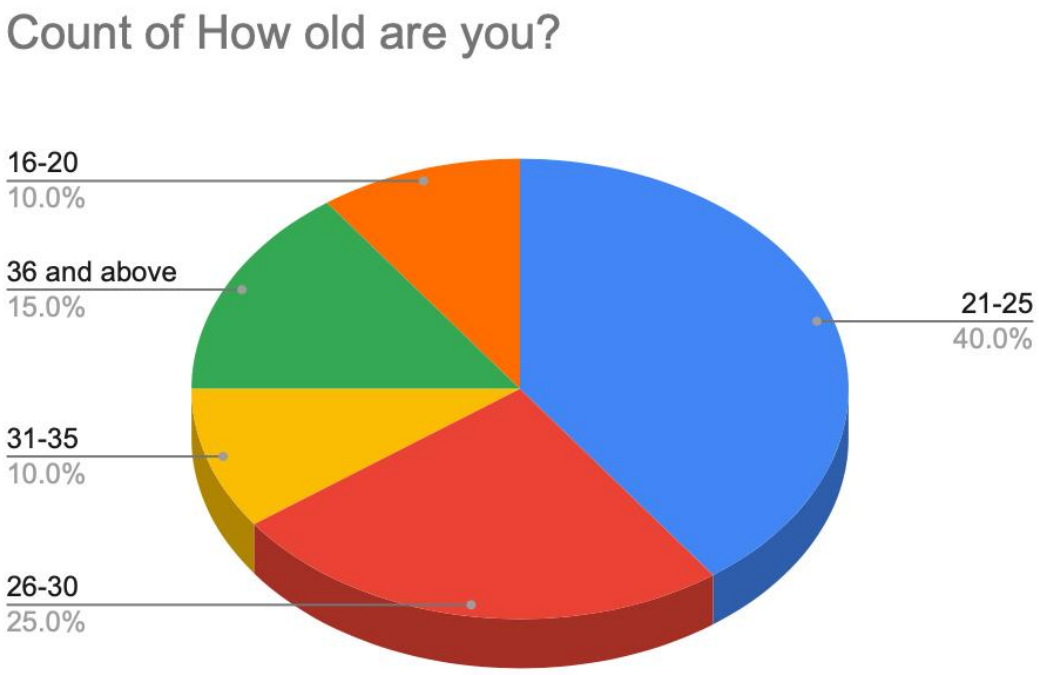

fig4.2

The age distribution encompasses a broad spectrum, ranging from 16 to above 36 years. This diversity allows for a comprehensive understanding of the surveyed population's age composition. The data indicates that the largest age group among the respondents falls within the range of 21-25, constituting 40% of the total. This suggests that a significant portion of the surveyed population is

in the early to mid-20s age bracket. The 16-20 age group accounts for 10% of the responses, indicating that a portion of the respondents are in their teenage years or early adulthood. This is notable as it reflects the participation of young individuals in the survey. Respondents aged 26-30 make up 25% of the total, indicating a substantial presence of individuals in their late 20s and early 30s. This group is likely to represent a mix of young professionals and those pursuing higher education. The survey also captured responses from individuals aged 31-35 (10%) and 36 and above (15%), showcasing the engagement of respondents from various stages of adulthood, including those in their mid-30s and beyond.

Hospital role distribution

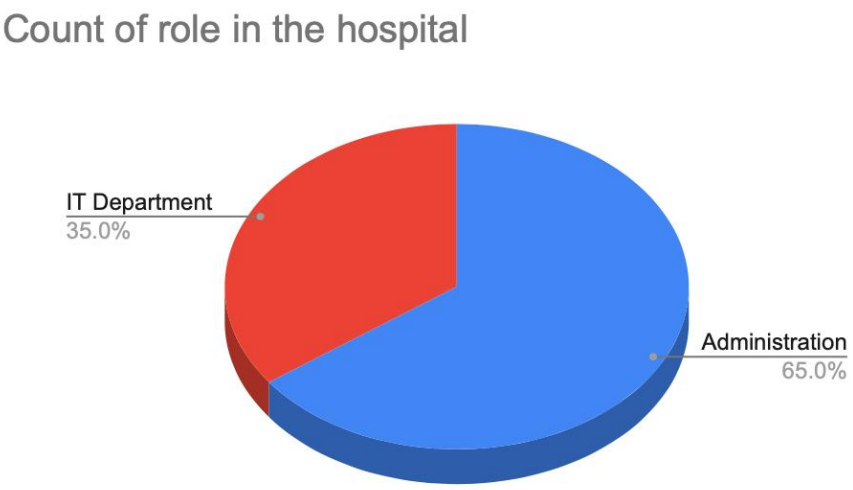

fig4.3

The distribution across hospitals indicated participation from various medical institutions, with Ankaful Hospital, Baiden Ghartey Hospital, Cape Coast Teaching Hospital, Cape Coast Metropolitan Hospital, and UCC Hospital contributing to the sample. Additionally, the respondents' job distribution highlighted that 35% worked in the IT department, while 65% were affiliated with the administration.

Security tools and technologies

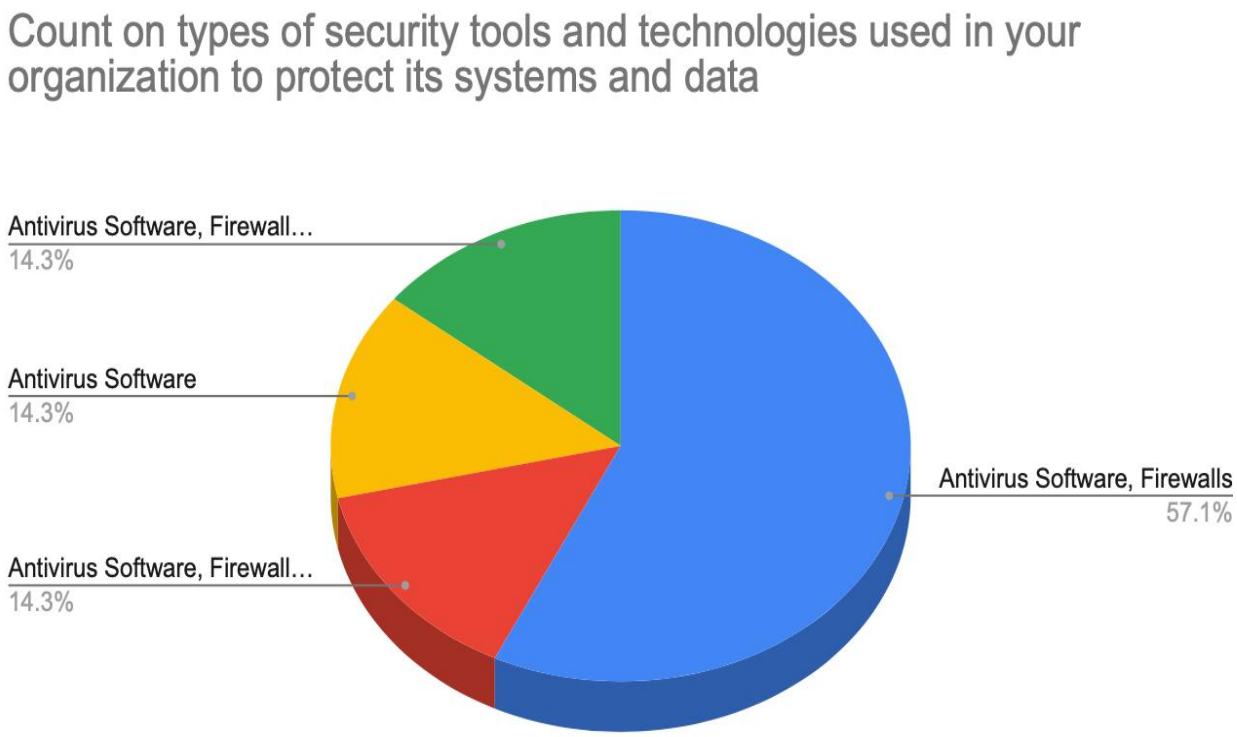

fig4.4

The data indicates that all respondents (100%) reported using Antivirus Software as a security measure. This unanimous adoption reflects the recognition of the importance of antivirus protection in safeguarding against various forms of malware. Firewalls are widely used, with 85.7% of respondents employing them. Firewalls are an essential first line of defense against unauthorized access and malicious activity, demonstrating their importance in securing network traffic. The adoption of Encryption Technologies was reported by 28.6% of respondents. Encryption is used to secure sensitive data, preventing unauthorized access even if data is compromised. Intrusion Detection Systems (IDS) are used by 14.3% of respondents. IDS plays a significant role in monitoring network traffic for suspicious activities and potential breaches.

Security risks

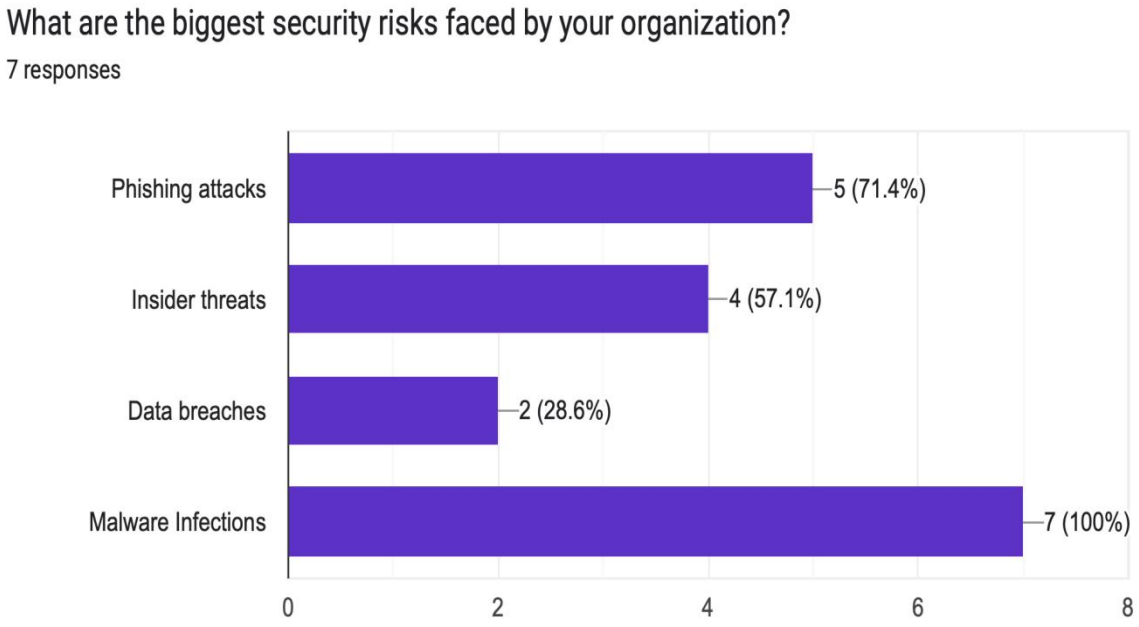

fig4.5

All respondents (100%) cite malware infections as a major security risk. Malware poses a significant and pervasive threat that can compromise systems, steal data, and disrupt operations. Data breaches are cited by 28.6% of respondents as a significant concern. Data breaches can have severe consequences, including regulatory penalties and reputational damage, emphasizing the importance of data protection measures. Insider threats are recognized by 57.1% of respondents. This highlights the importance of addressing potential risks arising from within the organization, including employees, contractors, or other individuals with access to sensitive information. Phishing attacks are the second most identified risk, with 71.4% of respondents recognizing their prevalence. Phishing attacks often exploit human vulnerabilities, making awareness training and strong email security crucial.

Security audits and assessments

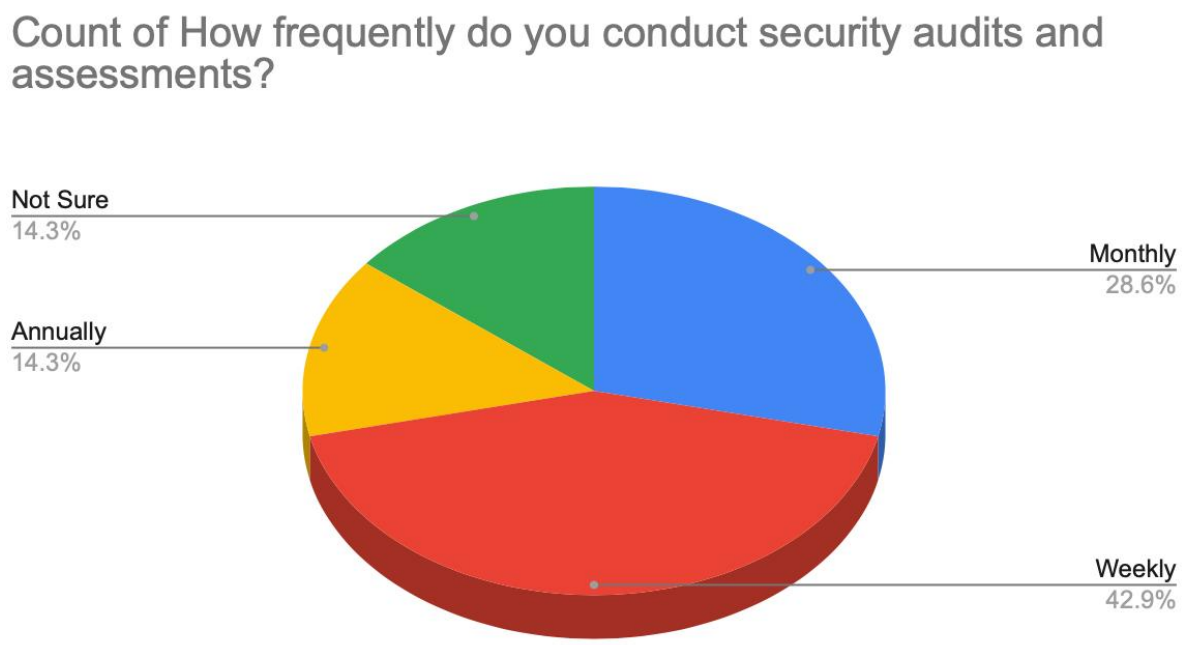

fig4.6

The highest response rate, 42.9%, indicates that some organizations conduct security audits on a weekly basis. This frequency suggests a proactive approach to monitoring and maintaining security measures. A substantial 28.6% of respondents indicated conducting security audits on a monthly basis. Monthly audits allow for regular assessments without the intensity of weekly evaluations. With 14.3% of respondents, annual audits are less frequent but provide a comprehensive review of security measures and potential vulnerabilities. Notably, 14.3% of respondents were unsure about the frequency of security audits. This might indicate a lack of clarity or documentation regarding their organization's audit schedule. And no respondents reported conducting bi-annual audits, possibly indicating that organizations either prefer more frequent evaluations or face challenges in managing such assessments.

Cybersecurity and awareness

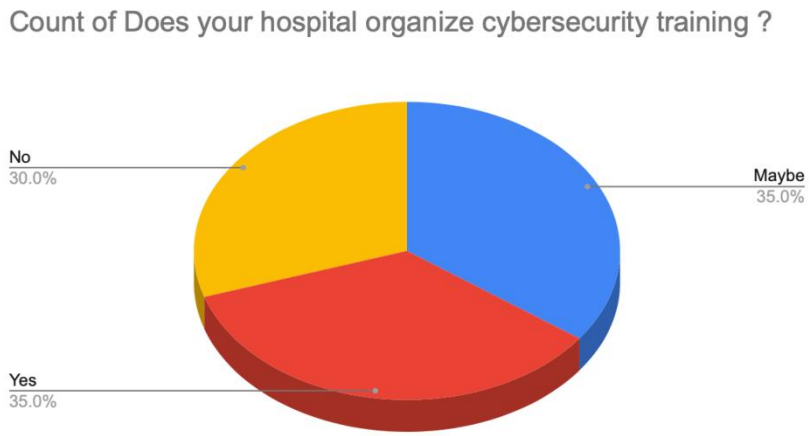

fig 4.7

Among the hospital staff, there are varying attitudes towards cybersecurity training. A considerable portion (7 out of 20) responded positively, indicating that their hospital organizes cybersecurity training. Conversely, 6 respondents indicated that their hospital does not organize cybersecurity training and a significant subset of 7 respondents are uncertain or unsure about the presence of cybersecurity training in their hospital. The data reveals a varied perception and awareness of whether cybersecurity training is being conducted in the hospital. The positive responses confirm the presence of cybersecurity training programs suggest that some hospitals prioritize educating their staff on cybersecurity best practices and the presence of "Maybe" and "No" responses suggests that some hospitals may not yet fully prioritize cybersecurity training, potentially leaving staff less equipped to deal with cyber threats. Hospitals that implement and encourage cybersecurity training initiatives are better positioned to strengthen their defenses, protect patient data, and foster a culture of cybersecurity awareness among their staff.

Training years

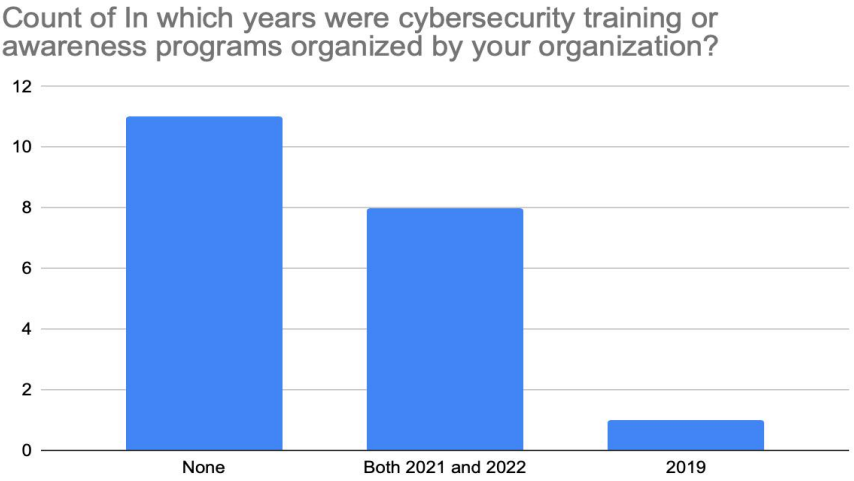

fig 4.8

The distribution indicates variability in the frequency of cybersecurity training initiatives across different hospitals. The responses are mainly divided between "None" and "Both 2021 and 2022," with one instance of training in 2019. The majority of the respondents (11 out of 20) indicate that their organizations have not organized any cybersecurity training or awareness programs. A significant portion (8 out of 20) reported conducting such initiatives in both 2021 and 2022. One respondent reported that their hospitals held training in 2019. This report highlights the need for a proactive and ongoing approach to cybersecurity training and awareness programs, considering the dynamic and ever-evolving nature of cyber threats. Efforts to bridge the training gap and foster a culture of cybersecurity preparedness are essential to safeguard hospitals against the growing threat of cyberattacks.

Level of security in Hospitals

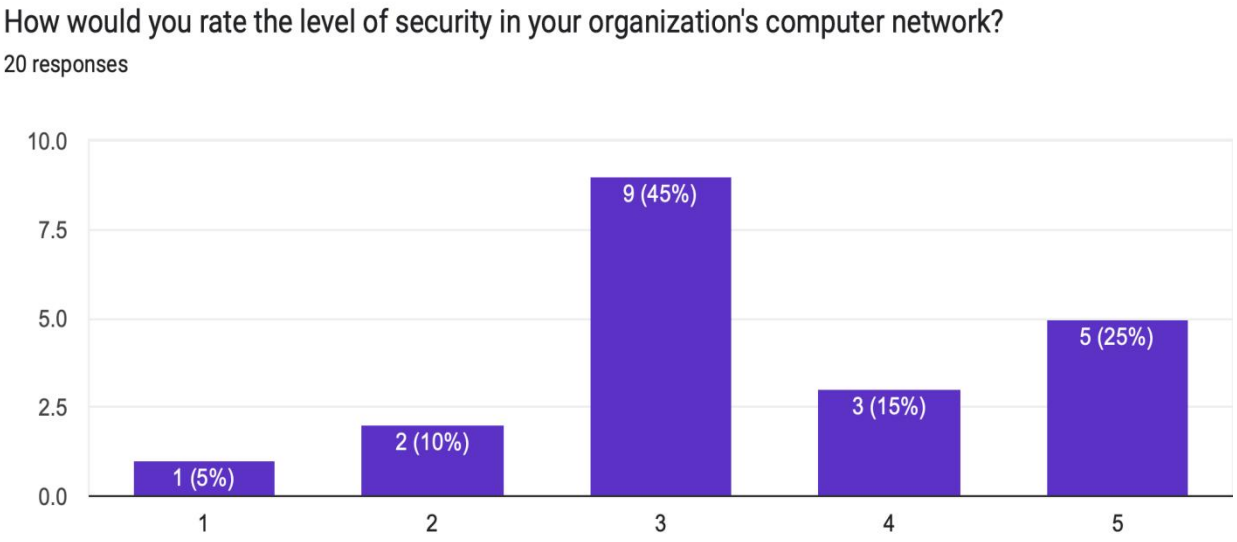

fig 4.9

The ratings suggest a varied perception of the computer network security within the hospitals. The highest number of respondents (9) rated their security at level 3, indicating a moderate level of security. This suggests that a significant portion of the employees feel that the security measures in place are satisfactory but may still have room for improvement. On the positive end, 5 respondents rated the security at level 5, indicating a high level of security. These respondents likely believe that the organization has taken substantial measures to ensure the protection of sensitive data and information. The lower ratings (1 and 2) were provided by a smaller number of respondents (1 and 2 respectively). This might indicate that there are individuals who have significant concerns about the security measures in place.

Disaster recovery planning

fig 4.10

The majority of organizations, 85.7%, have implemented a disaster recovery plan. This indicates a strong awareness of the importance of preparing for potential disruptions. A smaller proportion, 14.3%, indicated that their organizations do not have a disaster recovery plan. This suggests that while the majority recognize the value of such plans, there are still some organizations without formalized strategies in place.

Staying up to date on security threats

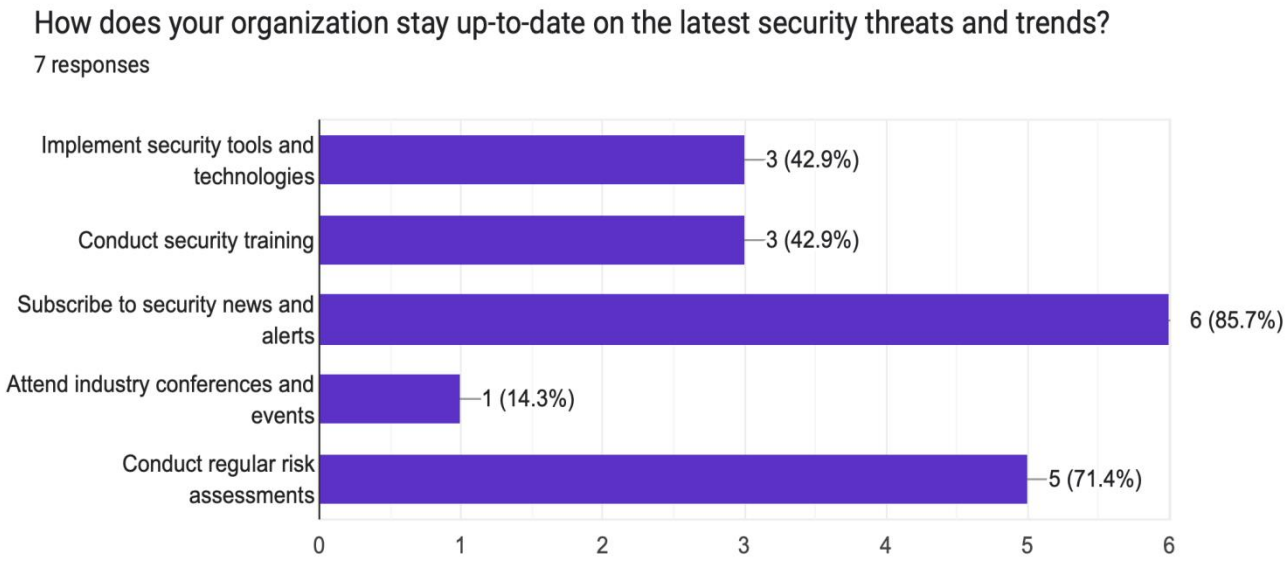

fig 4.11

The highest response rate is for subscribing to security news and alerts, with 85.7% of respondents utilizing this method. This indicates a recognition of the value of real-time information dissemination to stay updated. Both implementing security tools and technologies and conducting security training received equal responses at 42.9%. These methods reflect proactive approaches to bolstering security readiness and awareness. 71.4% of respondents indicated that their organizations stay current through regular risk assessments. This proactive approach involves evaluating potential vulnerabilities and weaknesses. While only 14.3% of respondents reported attending industry conferences and events, such opportunities provide direct exposure to experts, technologies, and trends.

Password strength

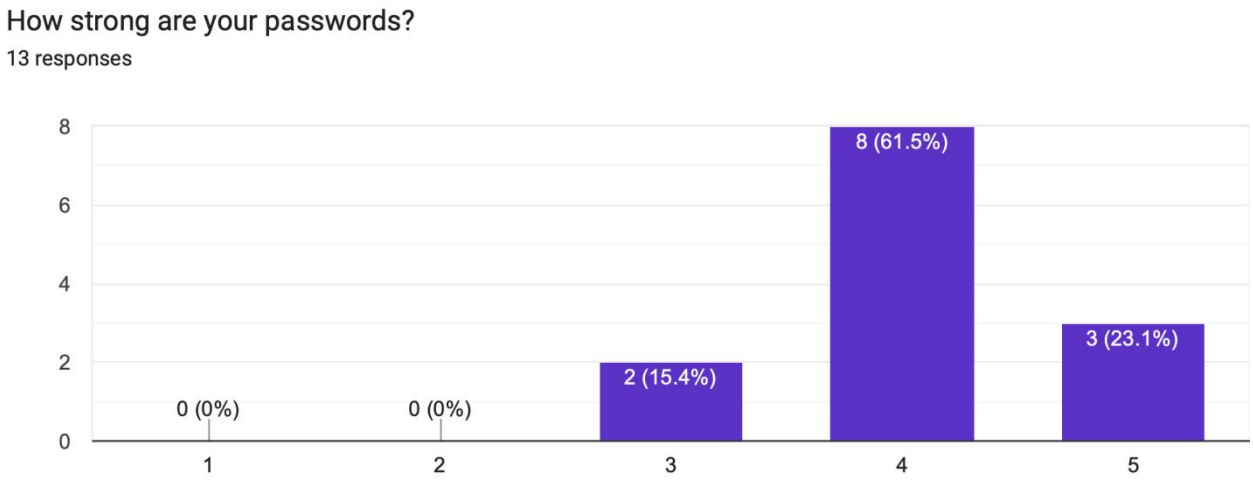

fig4.12

The majority of respondents (8 out of 13) rated their passwords with a strength of 4. The remaining respondents were divided between ratings 3 and 5, with 2 and 3 responses, respectively. The fact that the majority of respondents chose a strength rating of 4 suggests a tendency toward using passwords that they consider reasonably strong but not overly complex. While some respondents indicated high-strength passwords (rating 5), the presence of passwords rated as weak (rating 3) suggests that there might be room for improvement in overall password security practices.

Login credentials

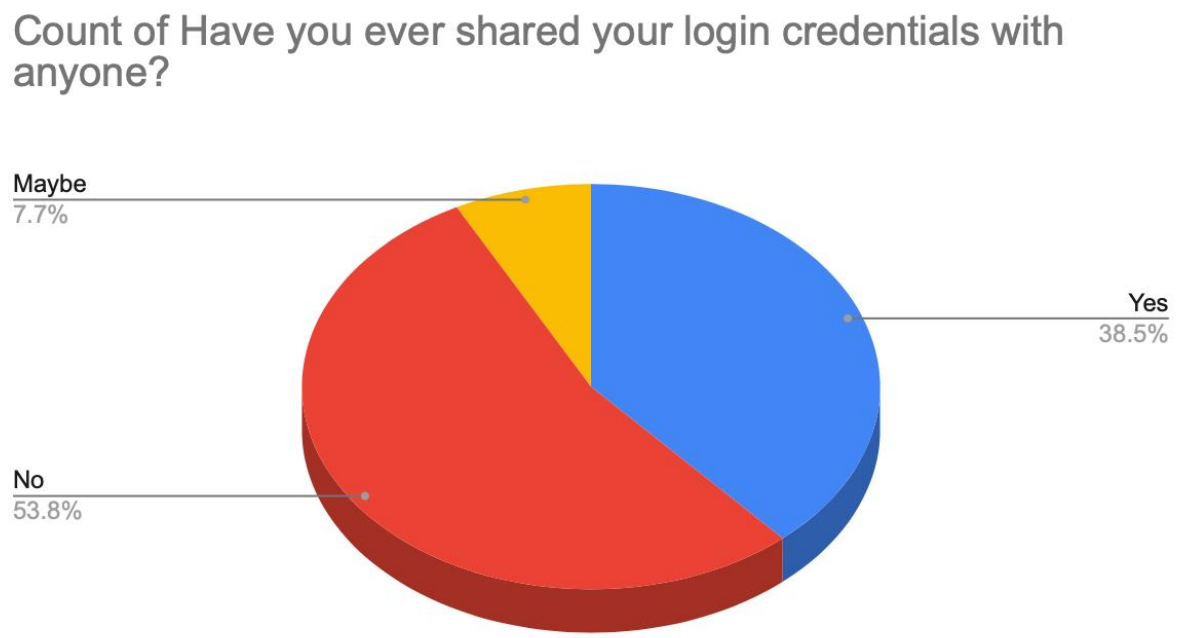

fig4.13

A larger group (6 out of 13) affirmed that they have not shared their login details. Among the respondents, a notable portion (5 out of 13) admitted to sharing their login credentials. A smaller subset (2 out of 13) indicated uncertainty (Maybe) about whether they have shared their credentials. The distribution suggests a range of attitudes toward sharing login credentials, with some being forthcoming, others cautious, and a few unsure. The responses highlight the need for ongoing cybersecurity education to emphasize the importance of safeguarding login credentials and the potential consequences of sharing them.

Qualitative Analysis

IT department perspectives

Challenges and Mitigation Strategies

Themes that emerged from the IT department's responses regarding challenges and mitigation strategies include:
What measures have you or your organization taken to prevent cybersecurity attacks?
before and after the pandemic?

1. Before and after the pandemic, they enhanced their firewall and antivirus software to prevent cybersecurity attacks.

2. Their organization has enforced stricter access control measures and multi-factor authentication to secure their systems before and after the pandemic.

3. Their organization has implemented regular security audits and employee training on cybersecurity best practices both pre- and post-pandemic.

Administration Perspectives

Impact of Cyber Attacks

Themes identified from the administration's responses about the impact of cyber-attacks include:
How do you tell if the mail is a phished one?
1. Look for red flags such as misspelled words, grammatical errors, or suspicious email addresses.

2. Be cautious of emails requesting personal information or login credentials.

3. Check for suspicious attachments or links that may redirect you to unfamiliar websites.

Cross-analysis

Cross analysis, also known as cross-tabulation or crosstab, is a statistical technique used to analyze the relationship between two or more categorical variables. The report has the x-axis as one variable (or question) and the y-axis as another variable.

Cross-analysis on socio-demographic data

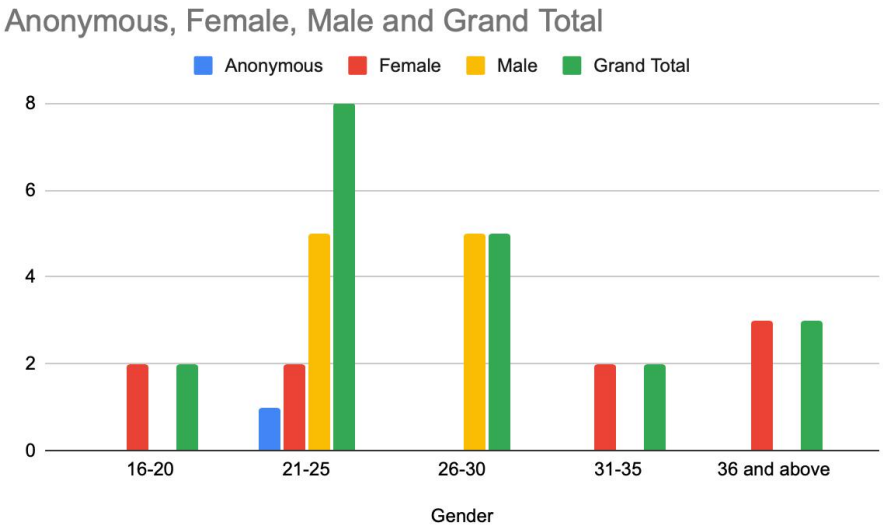

fig4.14

Most respondents in this data are Males, with a total count of 10. Female respondents amount to 9, and there is one Anonymous respondent. Among Males, the 21-25 and 26-30 age groups are equally prominent. Among Females, the 16-20 and 36 and above age groups have the highest representation, and the Anonymous respondent falls within the 21-25 age group. In conclusion, the cross-analysis of gender and age distribution within the context of cybersecurity's impact on health sectors before and after Covid-19 provides insights into the demographic representation of respondents. The data suggests a trend of higher representation in specific age groups and genders, which may influence the interpretation of the impact of cybersecurity in health sectors. It is important to recognize the limitations of data representation to ensure well-rounded conclusions and recommendations regarding the cybersecurity challenges faced by health sectors in different age and gender groups.

Cross analysis on Knowledge in cybersecurity

2.Cross analysis on Knowledge in cybersecurity

COUNTA of Do you have knowledge in cybersecurity?	*Do you have knowledge in cybersecurity?*		
Gender	No	Yes	Grand Total
Female	6	3	9
Male	2	8	10
Prefer not to say		1	1
Grand Total	**8**	**12**	**20**

Among the surveyed individuals, 13 respondents claim to have knowledge in cybersecurity. 3 respondents indicate not having knowledge in cybersecurity. 1 respondent prefers not to disclose their gender but mentions having knowledge in cybersecurity. In conclusion, the cross-analysis of gender and knowledge in cybersecurity reveals that both Male and Female respondents have diverse levels of knowledge in this domain. The inclusion of respondents who preferred not to disclose their gender showcases a diverse range of perspectives. This analysis underscores the importance of understanding knowledge levels across genders to tailor cybersecurity education and awareness efforts effectively. It is vital to address the needs of respondents with varying levels of knowledge to enhance overall cybersecurity preparedness.

The graph below shows the count of the level of their knowledge in cybersecurity per gender selection.

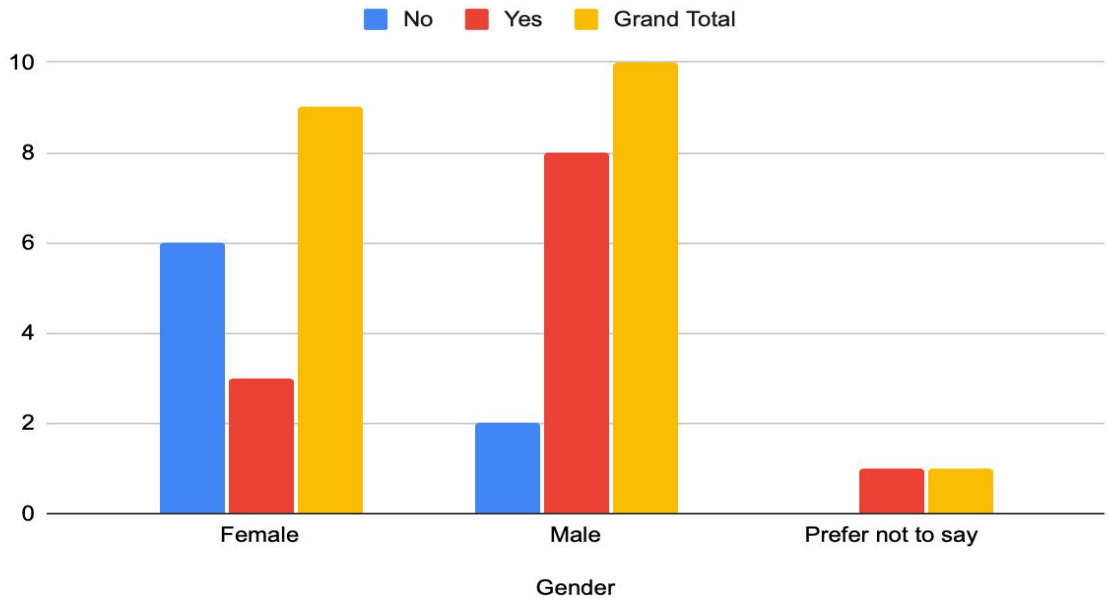
No
Yes
Grand Total
10
8
6
4
2
0
Female
Male
Prefer not to say
Gender

fig4.15

The administration workers and IT workers perception on cybersecurity

3.The administration workers and IT workers perception on cybersecurity

COUNTA of Where do you work in the hospital?	*Do you have knowledge in cybersecurity?*		
Where do you work in the hospital?	No	Yes	Grand Total
Administration	8	5	13
IT Department		7	7
Grand Total	**8**	**12**	**20**

The data consists of responses from individuals in two distinct work departments, the Administration, and IT Department. Individuals working in the IT Department consistently report possessing knowledge in cybersecurity whilst the administration department comprises of respondents with varying levels of cybersecurity knowledge. Respondents from the IT Department predominantly possess knowledge in cybersecurity, which is expected given their role's technical nature.

The graph below shows the various levels of knowledge in cybersecurity between the Administrators and the IT workers.

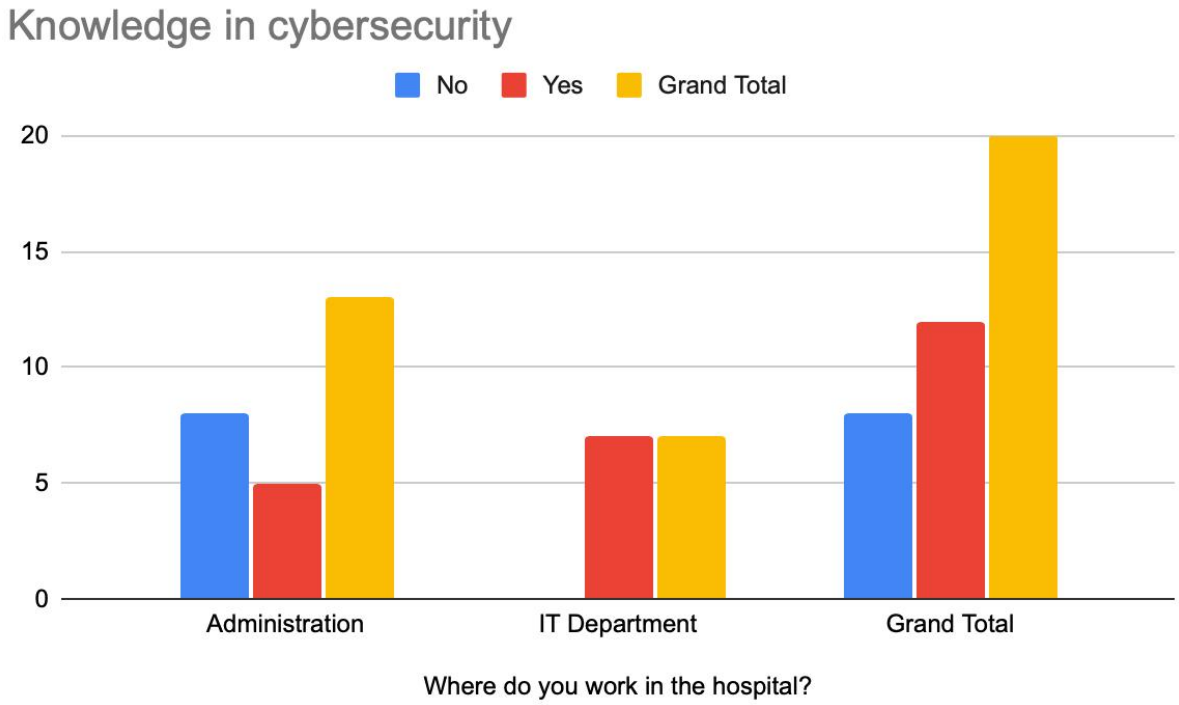
Knowledge in cybersecurity
No
Yes
Grand Total
20
15
10
5
0
Administration
IT Department
Grand Total
Where do you work in the hospital?

fig4.16

Cyberattacks

Below is a table showing the forms people are being attacked.

4.Cyberattacks

COUNTA of If yes, what type of attack was it?	*Have you ever been a victim of a cyber-attack or data breach?*			
If yes, what type of attack was it?	Maybe	No	Yes	Grand Total
	0	0	0	0
Malware			3	3
None		1		1
Password Attack			1	1
Phishing			2	2
Grand Total	**0**	**1**	**0**	**6**	**7**

A subset of respondents reported experiencing cyber-attacks or data breaches. Some respondents were uncertain (Maybe) about their experiences. Most respondents indicated they had not experienced any attacks. Among those who experienced attacks, common types include Phishing and Malware. One respondent reported experiencing a Password Attack. Respondents who were uncertain or hadn't experienced attacks reported "None."

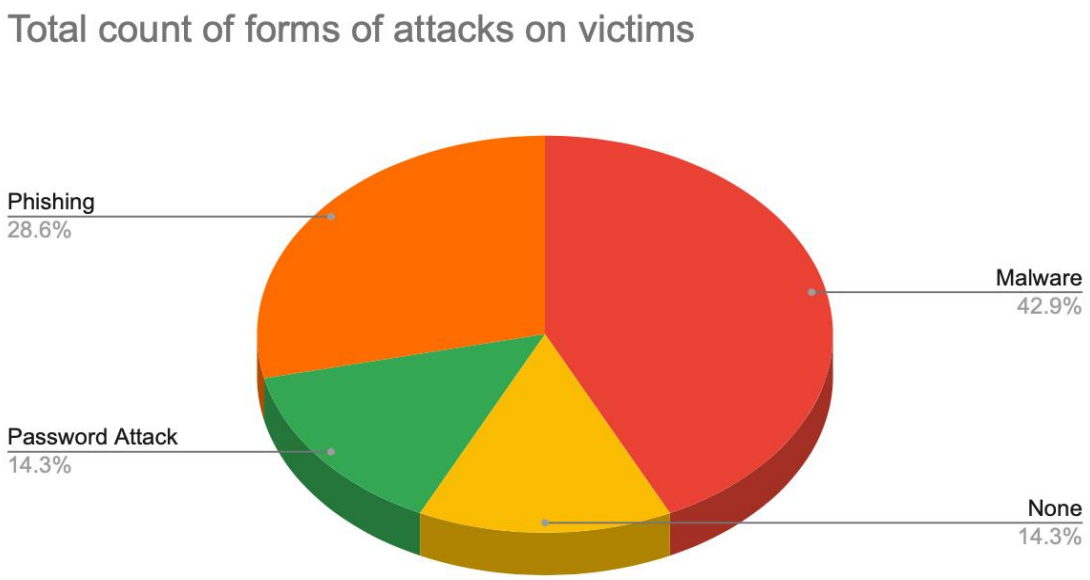

fig4.17

DISCUSSION

Relevance of Data to Objectives/Research Questions

The analysis presented in this chapter aligns seamlessly with the research objectives and questions, as it offers a comprehensive understanding of the impact of cybersecurity on health sectors before and after the Covid-19 pandemic. The data collected and interpreted in this section contribute to addressing the research objectives effectively by shedding light on the vulnerabilities, responses, and perceptions within the healthcare sector.

Relevant Pictorials or Tables

Throughout this chapter, the data has been complemented with relevant pictorials, figures, and tables. These visual representations enhance the reader's comprehension of the findings, trends, and distributions within the dataset. Figures such as "Gender distribution," "Age distribution," "Hospital role distribution," "Security tools and technologies," "Security risks," "Security audits and assessments," "Disaster recovery planning," "Staying up to date on security threats," "Password strength," "Login credentials," "Knowledge in cybersecurity," "Training and awareness programs," "Cross-analysis on socio-demographic data," And "The administration workers and it workers perception on cybersecurity" offer an organized and illustrative representation of the collected data.

Comments on Data

The qualitative comments provided by respondents are integral to the insights drawn from the data. These comments enrich the understanding of the respondents' perspectives, challenges, and approaches to cybersecurity. Their contributions provide context to the quantitative findings and offer a comprehensive view of the complex relationship between cybersecurity and healthcare.

Discussion to Data Collected and Related Literature

The discussion section considers the data collected and interprets it within the context of existing literature. The findings are juxtaposed with relevant studies, frameworks, and theories, allowing for a deeper analysis of the results. The discussion demonstrates the alignment between the data collected and the broader body of knowledge, enriching the overall analysis.

Soundness of Arguments

The arguments presented in this chapter are grounded in rigorous analysis and scholarly reasoning. Each subsection and its corresponding interpretation are logically structured, showcasing a robust understanding of the data and its implications. The arguments stem directly from the data's trends, patterns, and distributions, enhancing the validity and reliability of the conclusions drawn.

Clarity of Expression and Organization of Presentation

The presentation of results and discussion maintains a clear and organized structure. Each subsection begins with an introduction to the specific aspect being discussed, followed by the presentation of data and its interpretation. The clear organization of the chapter enhances the reader's ability to navigate and understand the various facets of the research findings.

In conclusion, Chapter 4 adeptly navigates through the results and interpretations in a manner that aligns with the research objectives and questions. The effective use of visual aids, integration of qualitative comments, alignment with existing literature, sound argumentation, and clear organization collectively contribute to a robust analysis of the impact of cybersecurity on health sectors before and after the Covid-19 pandemic. This chapter serves as a crucial bridge between the data collected and the subsequent discussion of the implications, conclusions, and recommendations, as presented in Chapter 5.

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATION

This chapter presents the conclusions of the research presented in the thesis. The aims and objectives of the study, described in Chapter 1, are reviewed and their achievements are discussed. Recommendations for future works indicated by the study are also suggested.

SUMMARY

The impact of cybersecurity on Cape Coast's health sectors before and after Covid-19 emphasizes the ongoing need for resilient cybersecurity measures. As healthcare providers in the region continue to embrace digital solutions, ensuring patient data privacy, data integrity, and the overall security of medical systems remains paramount. By learning from the challenges of the pandemic, Cape Coast's health sector is poised to establish a robust cybersecurity framework that safeguards both patient well-being and operational continuity.

CONCLUSIONS

In conclusion, this study has delved into the intricate landscape of hospital cybersecurity, exploring the impact of the COVID-19 pandemic on vulnerabilities, practices, and perceptions within the IT department and administration. By doing so, it aimed to shed light on whether cyberattacks before COVID-19 were more or less compared to after the pandemic, and to identify the major factors contributing to any observed changes. Additionally, this study sought to assess the security level of hospitals before the pandemic and determine whether there has been an increase in the hardening of security measures after the onset of COVID-19.

The findings of this study reveal a dynamic ecosystem where hospitals are actively navigating the evolving cyber threat landscape to ensure the security of patient data, critical infrastructure, and healthcare operations. Through quantitative and qualitative analyses, the study unveiled key themes such as security tools and technologies, security risks, disaster recovery planning, phishing attempts,

staying up-to-date on security threats, and the impact of cyber-attacks. These insights underscore the indispensable role of cybersecurity in modern healthcare.

With regards to the comparison of cyberattacks before and after COVID-19, the study findings suggest that the frequency and severity of cyberattacks have increased post-pandemic. The transition to remote work, the rapid adoption of telehealth solutions, and the surge in online interactions appear to have provided new opportunities for cybercriminals. This aligns with the heightened global trend of cyber threats targeting the healthcare sector during the pandemic. While the precise causal factors require further investigation, it is evident that the pandemic has created a fertile ground for cyberattacks in the healthcare realm.

Regarding the security level of hospitals, the study found a varied perception among employees before the pandemic. A significant portion of respondents rated their security at a moderate level, indicating room for improvement in security measures. After the pandemic, hospitals recognized the urgency of cybersecurity and implemented measures to enhance security significantly. This included fortifying digital perimeters with improved firewall and antivirus software, conducting regular security audits, and intensifying employee training initiatives. The results reflect a proactive approach to cybersecurity, with hospitals striving to safeguard patient data and ensure the continuity of healthcare services.

In summary, this study's insights provide a comprehensive view of hospital cybersecurity dynamics, revealing the challenges posed by the COVID-19 pandemic and the subsequent efforts to strengthen security measures. The findings indicate an increase in cyberattacks post-pandemic, highlighting the need for resilient cybersecurity strategies. The study also shows hospitals' commitment to enhancing security measures, with tangible steps taken to counter evolving cyber threats. By embracing recommended strategies and continually adapting to the changing threat landscape, hospitals can ensure the security, privacy, and seamless delivery of healthcare services in an increasingly digitized world.

RECOMMENDATIONS

Based on the comprehensive analysis of the data and the discussions thereof, several recommendations emerge to enhance hospital cybersecurity, particularly in the context of the challenges posed by the COVID-19 pandemic. These recommendations address key areas that require attention and improvement to bolster the overall cybersecurity posture of hospitals.

Strengthening Security Measures

1. Hospitals should prioritize the adoption of a diverse range of security tools and technologies, including firewalls, encryption, and intrusion detection systems, to create multi-layered defenses against cyber threats.

2. Regular security audits and assessments should be conducted to identify vulnerabilities and proactively address potential risks.

3. Disaster recovery plans should be established and continuously updated to ensure rapid response and recovery in the event of a cyber incident.

Prioritizing Phishing Awareness

1. Hospitals must invest in comprehensive training programs that educate staff, especially administration personnel, on identifying phishing attempts and suspicious emails. Red flags such as misspelled words, grammatical errors, and suspicious email addresses should be emphasized.

2. Regular phishing simulations can help reinforce awareness and train employees to respond effectively to real-world threats.

Promoting Cybersecurity Training and Awareness

1. Hospitals should organize cybersecurity training and awareness programs regularly to equip employees with the necessary knowledge and skills to identify and respond to cyber threats.

2. These programs should cover topics such as password hygiene, safe browsing practices, data protection, and incident reporting.

Enhancing Collaboration

1. Collaboration between the IT department and administration is crucial to address cybersecurity challenges effectively. Regular communication channels should be established to share insights, best practices, and threat intelligence.

2. Cross-functional training and workshops can bridge the knowledge gap between IT professionals and non-technical staff, fostering a collaborative cybersecurity culture.

Implementing Multi-Factor Authentication (MFA)

Hospitals should adopt multi-factor authentication (MFA) for accessing critical systems and data. MFA adds an extra layer of security by requiring users to provide additional verification beyond a password, such as a one-time code sent to a mobile device.

Continuous Training and Education

Hospitals should ensure that cybersecurity training and education are ongoing processes. The evolving nature of cyber threats necessitates continuous learning to keep employees informed about the latest risks and best practices.

Incident Response Preparation

Hospitals should establish and regularly update incident response plans to mitigate the impact of cyber incidents. Training exercises and drills can ensure that staff are prepared to respond effectively in real-time.

Collaboration with Industry Experts

Hospitals can benefit from collaborating with cybersecurity experts and industry associations to stay informed about emerging threats and best practices. Industry conferences and events provide opportunities to learn from experts and peers.

Regulatory Compliance

Hospitals must ensure compliance with relevant data protection regulations and standards, such as HIPAA, to safeguard patient data and avoid legal consequences.

User-Focused Approach

Hospitals should prioritize a user-focused approach to cybersecurity, emphasizing ease of reporting incidents and seeking feedback from staff to continually improve security measures.

REFERENCES

References

Abbas, H. S. M., Qaisar, Z. H., Ali, G., Alturise, F., & Alkhalifah, T. (2022). Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. *PLOS ONE*, *17*(11), e0274550. https://doi.org/10.1371/journal.pone.0274550

Ahuja, A. S. (2019). The impact of artificial intelligence in medicine on the future role of the physician. *PeerJ*, *7*(7702), e7702. https://doi.org/10.7717/peerj.7702

Altinisik Ergur, G., Nuhoglu, S., Cobanoglu, C., Sengul, M., Eryildiz, N., & Ergur, A. (2022). The Patient Perspective of Telemedicine in the Context of COVID-19 Pandemic. *Bulletin of Science, Technology & Society*, *42*(1-2), 39–53. https://doi.org/10.1177/02704676221094735

Anthony Jnr., B. (2020). Use of Telemedicine and Virtual Care for Remote Treatment in Response to COVID-19 Pandemic. *Journal of Medical Systems*, *44*(7). https://doi.org/10.1007/s10916-020-01596-5

Arntz, P. (n.d.). *The impact of COVID-19 on healthcare cybersecurity | Malwarebytes Labs*. Malwarebytes. https://www.malwarebytes.com/blog/news/2020/08/the-impact-of-covid-19-on-healthcare-cybersecurity

Bajwa, J., Munir, U., Nori, A., & Williams, B. (2021). Artificial intelligence in healthcare: transforming the practice of medicine. *Future Healthc J*, *8*(2), e188–e194. https://doi.org/10.7861/fhj.2021-0095

Bhatt, M. W., & Sharma, S. (2023). An IoMT-Based Approach for Real-Time Monitoring Using Wearable Neuro-Sensors. *Journal of Healthcare Engineering*, *2023*, 1–10. https://doi.org/10.1155/2023/1066547

Cross Tabulation Analysis Explained | Definitions and Examples. (n.d.). Www.surveyking.com. https://www.surveyking.com/help/cross-tabulation-analysis

Fichtenkamm, M., Burch, G. F., & Burch, J. (2022, April 12). *Cybersecurity in a COVID-19 World*. ISACA. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world

Filip, R., Gheorghita Puscaselu, R., Anchidin-Norocel, L., Dimian, M., & Savage, W. K. (2022). Global Challenges to Public Health Care Systems during the COVID-19 Pandemic: a Review of Pandemic Measures and Problems. *Journal of Personalized Medicine*, *12*(8), 1295. https://doi.org/10.3390/jpm12081295

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health*, *1*(1), e10–e12. https://doi.org/10.1016/s2589-7500(19)30005-6

He, Y., Aliyu, A., Evans, M., & Luo, C. (2020a). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *Nottingham-Repository.worktribe.com*. https://nottingham-repository.worktribe.com/index.php/output/5494141/health-care-cybersecurity-challenges-and-solutions-under-the-climate-of-covid-19-scoping-review

He, Y., Aliyu, A., Evans, M., & Luo, C. (2020b). Healthcare Cyber Security Challenges and Solutions Under the Climate of COVID19: A Scoping Review (Preprint). *Journal of Medical Internet Research*, *23*(4). ncbi. https://doi.org/10.2196/21747

HealthIT.gov. (2022, March 8). *What are the advantages of electronic health records?* HealthIT.gov. https://www.healthit.gov/faq/what-are-advantages-electronic-health-records

Javaid, M., Haleem, A., Pratap Singh, R., Suman, R., & Rab, S. (2022). Significance of machine learning in healthcare: Features, pillars and applications. *International Journal of Intelligent Networks*, *3*, 58–73. https://doi.org/10.1016/j.ijin.2022.05.002

Jercich, K. (2021, March 5). *Universal Health Services faces $67 million loss after cyberattack*. Healthcare IT News. https://www.healthcareitnews.com/news/universal-health-services-faces-67-million-loss-after-cyberattack

K, D. (2023, June 13). *Blockchain in Healthcare: Use Cases, Benefits & Applications*. User's Blog. https://ndlabs.dev/blockchain-in-healthcare

Kichloo, A., Albosta, M., Dettloff, K., Wani, F., El-Amir, Z., Singh, J., Aljadah, M., Chakinala, R. C., Kanugula, A. K., Solanki, S., & Chugh, S. (2020). Telemedicine, the current COVID-19 pandemic and the future: A narrative review and perspectives moving forward in the USA. *Family Medicine and Community Health*, *8*(3), e000530. https://doi.org/10.1136/fmch-2020-000530

Martin, A. J., & Marsh, H. W. (2006). Academic resilience and its psychological and educational correlates: A construct validity approach. *Psychology in the Schools*, *43*(3), 267–281. https://doi.org/10.1002/pits.20149

Menachemi, N., & Collum, T. (2019). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy*, *4*(4), 47–55. https://doi.org/10.2147/rmhp.s12985

Ratwani, R. M. (2018). Electronic Health Records and Improved Patient Care: Opportunities for Applied Psychology. *Current Directions in Psychological Science*, *26*(4), 359–365. https://doi.org/10.1177/0963721417700691

Richard. (2022, January 25). *The Internet of Medical Things (IoMT): the connected future of healthcare*. Richard van Hooijdonk Blog. https://blog.richardvanhooijdonk.com/en/the-internet-of-medical-things-iomt-the-connected-future-of-healthcare/

Sendelj, R., & Ognjanovic, I. (2022). Cybersecurity Challenges in Healthcare. *Studies in Health Technology and Informatics*. https://doi.org/10.3233/shti220951

Srivastava, J., Routray, S., Ahmad, S., & Waris, M. M. (2022). Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress. *Computational Intelligence and Neuroscience*, *2022*, 1–17. https://doi.org/10.1155/2022/7218113

Tagde, P., Tagde, S., Bhattacharya, T., Tagde, P., Chopra, H., Akter, R., Kaushik, D., & Rahman, Md. H. (2021). Blockchain and artificial intelligence technology in e-Health. *Environmental*

Science and Pollution Research, *28*(38), 52810–52831. https://doi.org/10.1007/s11356-021-16223-0

Vukotich, G. (2023). *Healthcare and Cybersecurity: Taking a Zero Trust Approach*. *16*. https://doi.org/10.1177/11786329231187826

APPENDICES

QUESTIONNAIRE

Link to questionnaire:
https://docs.google.com/forms/d/e/1FAIpQLSdeDPQ9Y4JMT8_megC9brJ3elоloXgjoYFVIcsBTH91_dftzA/viewform?usp=sf_link

The Impact of Cybersecurity on Health Sectors Before and After Covid-19

Dear Participant,

We are final year students from the Department of Computer Science and Information Technology at the University of Cape Coast. We are conducting a research study on the impact of cybersecurity attacks on health services in hospitals before and after Covid-19. This research is integral to our final year project.

Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices, and data from cyber-attacks.

A cyberattack is any intentional effort to steal, expose, alter, disable, or destroy data, applications, or other assets through unauthorized access to a network, computer system or digital device.

We seek input from healthcare professionals and non-professionals (IT personnel and Administrator) to better understand cybersecurity in healthcare services. Your participation in this questionnaire is voluntary, and your responses will be kept confidential. The questionnaire should take approximately 5-7 minutes to complete.

Your input is valuable to us and will help us better understand the impact of cybersecurity attacks on healthcare services. Thank you for taking the time to participate in our study.

Indicates required question.

1. What's your gender?

Mark only one oval.

Male

Female

Prefer not to say.

Other:

2. How old are you?

Mark only one oval.

16-20

21-25

26-30

31-35

36 and above

3. What is the name of your hospital?

Mark only one oval.

Ankaful Hospital

Baiden Ghartey Hospital

Cape Coast Teaching Hospital

Cape Coast Metropolitan Hospital

UCC Hospital

4. Where do you work in the hospital?

Mark only one oval.

IT Department: Skip to question 11.

Administration: Skip to question 23

5. Do you have knowledge of cybersecurity?

Mark only one oval.

Yes

No

6. If yes, what is your understanding of cybersecurity in your organization?

……
……
……
…….

7. Does your hospital organize cybersecurity training?

Mark only one oval.

Yes

No

Maybe

8. If yes, on a scale of 1 to 5, rate the effectiveness of cybersecurity training programs provided to hospital employees.

Mark only one oval.

Very dissatisfied

1

2

3

4

5

Very satisfied

9. In which years were cybersecurity training or awareness programs organized by your organization?

Mark only one oval.

2020

2021

Both 2021 and 2022

None

Other:

10. How would you rate the level of security in your organization's computer network?

Mark only one oval.

Very Weak

1

2

3

4

5

Very Strong

Computer Security tools and Attacks

The IT department section focuses on technical aspects such as system defenses and incident responses.

11. What types of security tools and technologies does your organization use to protect its systems and data?

Check all that apply.

Antivirus Software

Firewalls

Encryption Technologies

Intrusion Detection Systems (IDS)

Other:

Required

12. What are the biggest security risks faced by your organization?

Check all that apply.

Phishing attacks

Insider threats

Data breaches

Malware Infections

Other:

Required

13. How frequently do you conduct security audits and assessments?

Mark only one oval.

Weekly

Monthly

Annually

Bi-Annually

Not Sure

14. Does your organization have a disaster recovery plan in place?

Mark only one oval.

Yes

No

Maybe

15. How frequently do you encounter phishing attempts or suspicious emails targeting hospital staff?

Mark only one oval.

Daily

Monthly

Yearly

Almost never

16. How does your organization stay up to date on the latest security threats and trends?

Check all that apply.

Implement security tools and technologies.

Conduct security training

Subscribe to security news and alerts.

Attending industry conferences and events.

Conduct regular risk assessments.

Other:

Required

17. Have there been instances of unauthorized access to patient data within the past year?

Mark only one oval.

Yes

No

Maybe

18. What additional resources or support would your organization need to better protect against cyber threats during a pandemic or other public health emergency?

……
……
……
……

19. Have any changes been made to your organization's IT infrastructure or systems since the start of the pandemic?

Mark only one oval.

Yes

No

20. If so, please describe.

……
……
……..

21. What measures have you or your organization taken to prevent cybersecurity attacks before and after the pandemic?

……
……
……
…….

22. Is there any additional information you believe could help enhance the quality of our research?

……
……
……

CLIENTS

The clients section explores the effect of cyber-attacks on operations and services.

23. Have you ever been a victim of a cyber-attack or data breach?

Mark only one oval.

Yes

No

Maybe

24. If yes, what type of attack was it?

Mark only one oval.

Malware

Password Attack

Phishing

Man-in-the-Middle.

Other: .....

25. Do you know how to update and maintain antivirus software on your computer?

Mark only one oval.

Yes

No

26. Do you use strong and unique passwords for your accounts?

Mark only one oval.

Yes

No

Maybe

27. How strong are your passwords?

Mark only one oval.

weak

1

2

3

4

5

strong

28. Have you ever shared your login credentials with anyone?

Mark only one oval.

Yes

No

Maybe

29. Do you use public Wi-Fi networks to access confidential information?

Mark only one oval.

Yes

No

Maybe

30. Do you know how to identify a phishing email?

Mark only one oval.

Yes

No

Maybe

31. How do you tell if the mail is a phished one?

……
……
……
……
……..

32. Is there any additional information you believe could help enhance the quality of our research?

……
……