Department of Electronic Engineering,
School Of Engineering, Physical and Mathematical Sciences

The Human Firewall: Strengthening Cybersecurity in Healthcare through Project Manager Training

Candidate Number: 2004403

A Dissertation Submitted
in Partial Fulfilment of the
Requirements for the Degree

MSc in Cybersecurity Project Management

Supervisor: Richard Granger

28th August, 2024

Author’s Declaration

It is declared that I am the sole author of this thesis. It is the actual copy of the dissertation that was accepted by my supervisor(s) including any necessary revisions. I also grant Royal Holloway University of London permission to reproduce and distribute electronic or paper copies of this project report.

2004403

28 August 2024

Abstract

The purpose of this research is to examine how cybersecurity training affects the behaviour of medical project managers and enhances security measures across healthcare organizations. The prevalence of networked medical equipment and digital health records render the healthcare industry uniquely susceptible to cyber-attacks, which can result in severe consequences including financial loss or reputation damage. Despite advancements in electronic health record systems and security procedures, challenging issues such as inadequate staff education and crisis management plans continue to afflict healthcare facilities.

Using a mixed-methods approach, this study combined quantifiable data from surveys with subjective insights derived from interviews conducted among medical project managers and cybersecurity experts. The quantitative information gathered through the survey was subjected to descriptive statistical analyses while thematic analysis was applied in assessing responses obtained during interviews.

The findings reveal that cybersecurity awareness training positively affects project managers' conduct and bolsters organizational security. Nevertheless, obstacles like limited time availability, inadequacy of pertinent instructional resources, and trouble relating knowledge to practical situations remain prevalent. To enhance the efficacy of cyber safety education efforts, custom-tailored content along with interactive instruction techniques are suggested alongside frequent sessions featuring continuous reinforcement supplemented by stronger leadership backing.

To sum up, this study highlights the crucial requirement for improved cybersecurity education among medical project managers in healthcare. Through tackling the recognized obstacles and adopting suggested enhancements, health institutions can bolster their security stance and safeguard confidential patient information.

Acknowledgements

In memory of Eloise, my feline companion of nearly eight years. Your spirited personality and unique features brought joy and companionship through numerous relocations. While your passing is mourned, the memories we shared endure. This work is dedicated in your honour.

To Richard Grainger, with sincere gratitude for your unwavering guidance and support throughout this journey. Your expertise, patience, and encouragement were instrumental in shaping this dissertation. Thank you for sharing your knowledge and inspiring my growth.

Research Ethics Approval

EE PGT - RESEARCH ETHICS COMMITTEE REVIEW OUTCOME	
Student Name:	**Wendi Soto**
Student ID:	100998355
Course Title/Year/Cohort (Sep or Jan)	CyberSecurity PM/2023/Sep
Title:	
What communication strategies can project managers utilize to effectively engage healthcare staff with varying technical backgrounds on cybersecurity threats and best practices?	
Summary of the Research Activity: (As documented by student in Research Ethics Form)	
This research explores how project managers in healthcare can effectively communicate cybersecurity to staff with varying technical skills. Surveys and interviews will identify preferred communication channels and strategies for fostering a more cybersecurity-aware healthcare workforce.	
Points Raised by Committee (If needed more clarity from student)	
1. 2. 3.	4. 5. 6.
Questions for the Student: (If conflict of interest exists and needed more clarity from student)	
1	
2	
3	
Risks involved in this Research: (According to EE PGT REC)	

For EE PGT Research Ethics Committee Only

Student Name and Number:	Wendi Soto 100998355
Decision:	**Approved:** 27th June 2024 **Provisional Approval:** *(Based on Meeting Specified Condition)*

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AI: Artificial Intelligence

CML: Cyber Maturity Level

CRM: Cybersecurity Risk Management

EHR: Electronic Health Record

GDPR: General Data Protection Regulation

HIPAA: Health Insurance Portability and Accountability Act

ICF: Informed Consent Form

IT: Information Technology

IoT: Internet of Things

ML: Machine Learning

PMT: Protection Motivation Theory

SCT: Social Cognitive Theory

TPB: Theory of Planned Behaviour

TES: Training Effectiveness Score

TRS: Training Relevance Score

U.S.: United States

List of Symbols

Σ= Sum

United Nations Sustainable Development Goals

This research aligns with several United Nations Sustainable Development Goals (SDGs), particularly:

- **SDG 3: Good Health and Well-being:** This research aims to improve healthcare project managers' awareness of cybersecurity measures, ultimately preventing data breaches and safeguarding patient safety and privacy. In doing so, it seeks to advance overall health outcomes.
- **SDG 9: Industry, Innovation, and Infrastructure:** Innovative approaches to cybersecurity training contribute to the growth of robust infrastructure within the healthcare industry.
- **SDG 16: Peace, Justice, and Strong Institutions:** The research indirectly supports this goal by helping to protect healthcare institutions from cyberattacks, thus ensuring their stability and the trust they engender.
- **SDG 17: Partnerships for the Goals:** Global partnerships are crucial in attaining the SDGs, as indicated by the emphasis placed on collaboration among healthcare organizations, cybersecurity experts and project managers.

Furthermore, this study indirectly enhances the achievement of SDG 4 (Quality Education) and SDG 8 (Decent Work and Economic Growth). Through its emphasis on ongoing education in cybersecurity and advocacy for a secure healthcare industry, it promotes a more sustainable and equitable futur

Chapter 1

Introduction

1.1 Background Information

Globally, cyber threats have become a growing concern for the healthcare industry due to its vulnerability. Networked medical devices and digital health records that are relied upon in this sector provide hackers with multiple opportunities to infiltrate systems (IBM Security, 2023). The ramifications of security breaches can be devastating as personal patient data may be lost or stolen leading to financial losses while gravely damaging the reputation of healthcare organizations (HHS, 2023). Notably, recent ransomware attacks on Universal Health Services highlight an urgent need for improved cybersecurity measures within the industry (Verizon, 2023). Healthcare organizations still have significant shortcomings despite the progress made in electronic health record (EHR) systems and security protocols. These weaknesses include insufficient staff training, inadequate incident response plans, and a shortage of customized security solutions (HIMSS, 2023). Table 1 demonstrates the escalating incidence and gravity of healthcare data breaches, as evidenced by the extent of impact on individuals. These top 15 U.S.-based breaches are an indication of how significant this issue has become (Hippa Journal).

Top 15 Healthcare Data Breaches in the U.S. (by Individuals Affected)

Rank	*Name of Covered Entity*	*Year*	*Covered Entity Type*	*Individuals Affected*	*Type of Breach*
1	Anthem Inc.	2015	Health Plan	78,800,000	Hacking/IT Incident
2	American Medical Collection Agency	2019	Business Associate	26,059,725	Hacking/IT Incident
3	Welltok, Inc.	2023	Business Associate	14,762,475	Hacking/IT Incident
4	Kaiser Foundation Health Plan, Inc.	2024	Health Plan	13,400,000	Unauthorized Access/Disclosure
5	Optum360, LLC	2019	Business Associate	11,500,000	Hacking/IT Incident

6	HCA Healthcare	2023	Business Associate	11,270,000	Hacking/IT Incident
7	Premera Blue Cross	2015	Health Plan	11,000,000	Hacking/IT Incident
8	Laboratory Corporation of America Holdings dba LabCorp	2019	Healthcare Provider	10,251,784	Hacking/IT Incident
9	Excellus Health Plan, Inc.	2015	Health Plan	9,358,891	Hacking/IT Incident
10	Maximus, Inc.	2023	Business Associate	9,179,226	Hacking/IT Incident
11	Perry Johnson & Associates, Inc., which does business as PJ&A	2023	Business Associate	8,952,212	Hacking/IT Incident
12	Managed Care of North America (MCNA)	2023	Business Associate	8,861,076	Hacking/IT Incident
13	Community Health Systems Professional Services Corporations	2014	Healthcare Provider	6,121,158	Hacking/IT Incident
14	PharMerica Corporation	2023	Healthcare Provider	5,815,591	Hacking/IT Incident
15	Science Applications International Corporation (SA	2011	Business Associate	4,900,000	Loss

Table 1
Source: The Hippa Journal

1.2 Significance and Motivation

As cyber threats targeting healthcare continue to increase, this study aims to address a significant knowledge gap: improving the cybersecurity proficiency of project managers operating within the industry. Recognizing their vital function in guaranteeing thriving implementation and management of healthcare initiatives, our study strives to empower them as committed promoters for cybersecurity by integrating comprehensive security measures into every stage - beginning from ideation up until completion- of each project.

1.2.1 Personal Motivation

Having a clinical science and healthcare background, I have witnessed the pivotal part project managers play in ensuring triumph for healthcare organizations. While overseeing an EHR system's launch at one organization, it was evident that these vital individuals possessed limited familiarity with cybersecurity best practices. Consequently, this deficiency triggered implementation delays while delicately risking patient data exposure to potential threats. My encounters emphasized how managing intricate medical projects can be challenging—particularly when dealing with delicate patient information and regulatory prerequisites—prompting my interest in discovering ways to improve outcomes by imparting advanced cybersecurity knowledge among medical project managers capable of mitigating risks significantly.

1.2.2 Broader Significance

The management of cybersecurity risks, also known as Cybersecurity Risk Management (CRM), poses a significant challenge to the healthcare industry. This study seeks to address and fill crucial gaps in CRM by underscoring the essential role played by medical project managers. It analyses the present state of security awareness within healthcare organizations while concentrating on areas that require improvement. The goal is to offer feasible recommendations aimed at bolstering cybersecurity practices for such establishments.

1.3 Aims and Objectives

The objective of this study is to assess how cybersecurity training aimed at promoting awareness can influence the conduct of medical project managers, as well as enhance healthcare organizations' general security measures. The objectives of this research are:

1. To identify specific cybersecurity risks faced by healthcare organizations.
2. To assess the current level of cybersecurity awareness among medical project managers.
3. To determine the effectiveness of existing cybersecurity training programs.
4. To develop recommendations for improving cybersecurity training tailored to medical project managers.

1.3.1 Research Question

The central research question guiding this study is: How does cybersecurity awareness training influence the behaviour of medical project managers and contribute to the overall security posture of healthcare institutions?

To address this central question, several sub-questions are explored:

1. How does cybersecurity awareness training specifically alter the conduct of medical project managers and enhance security practices within their projects?
2. Beyond individual behaviour change, how does training contribute to transforming the overall security culture within healthcare organizations?
3. What are the most effective methods for assessing the impact of cybersecurity awareness training on both individual behaviour and organizational security outcomes?

This study seeks to conduct a thorough analysis of cybersecurity awareness training in healthcare by delving into these sub-questions. The ultimate objective is to proffer valuable insights for crafting tailored training programs that can transform individual behaviour and enhance the overall cyber safety stance of medical establishments.

1.4 Methodology

To compile and examine data, our research employed a blend of qualitative and quantitative techniques through mixed methods. Medical project managers were interviewed using semi-structured protocols, while online surveys also helped in collecting information. Quantitative analysis techniques such as descriptive statistics were employed for survey data while the interview transcripts underwent thematic analysis for a more comprehensive understanding of the findings.

1.5 Report Outline

The focus of this study is the healthcare industry which covers hospitals, clinics, providers of medical equipment and supplies as well as healthcare professionals. Its objective is to enhance cybersecurity consciousness among project managers in healthcare by acknowledging the specific hurdles and regulatory obligations of this industry while aiming for better evaluation processes. This section outlines the structure of the dissertation:

Chapter One: Provides an overview of the study, including the background, significance, aims, objectives, scope, and methodology.

Chapter Two: This article examines the literature regarding cybersecurity threats within healthcare, assesses how project managers can mitigate these risks, and evaluates current training programs in place for cybersecurity.

Chapter Three: Outlines the methodology of research, encompassing aspects such as research design, the participants involved in the study population, techniques used for sampling them and gathering relevant data. Further topics include procedures followed to analyse captured information along with considering ethical implications that must be considered alongside limitations encountered during such endeavours.

Chapter Four: Presents the findings, analysis, and discussions. It explores the implications of the research findings for each research objective and summarizes the key insights.

Chapter Five: Concludes the dissertation, providing a summary of the research, conclusions based on the findings, and practice.

Chapter 2

Literature Review

2.1 Background and Significance

The purpose of this study, as described in Chapter 1, is to analyse the influence of cybersecurity awareness training on medical project managers and healthcare institutions' overall security stance. To accomplish our objective, we will explore the current state of cybersecurity threats within healthcare and scrutinize how project managers can reduce these hazards while also assessing already-implemented instructional programs.

2.2 Selection of Sources

A systematic exploration of the existing levels of cybersecurity awareness training among project managers in medical fields was pursued by carrying out a literature review through credible academic databases such as IEEE Xplore, Google Scholar, and PubMed. The search criteria comprised phrases like "cybersecurity awareness," "project management," "healthcare," "training efficiency" and "behavioural modification". Only peer-reviewed articles published between 2010 and 2024 were taken into account to narrow down the scope.

This study placed significant emphasis on empirical evidence of the efficiency of cybersecurity awareness training programs and common obstacles confronted by healthcare project managers. Additionally, reliable industry reports and white papers from organizations like HIMSS and ISACA were consulted to better understand current trends and optimal practices. Key resources for this research included foundational studies such as Al-Qahtani & Higgins' (2013) investigation into behaviour modification resultant from education initiatives.

2.3 Literature Review Rationale

To gain a comprehensive understanding of the current state of cybersecurity awareness training among medical project managers, I conducted a systematic review of the literature using reputable academic databases like PubMed, IEEE Xplore, and Google Scholar. The search terms included "cybersecurity awareness," "project management," "healthcare,"

"training effectiveness," and "behaviour change." The scope was limited to peer-reviewed articles published in English between 2010 and 2024.

I prioritized empirical evidence on the effectiveness of cybersecurity awareness training programs and challenges faced by healthcare project managers. Industry reports and white papers from reputable organizations like HIMSS and ISACA provided insights into current trends and best practices. Foundational studies, such as Al-Qahtani & Higgins (2013), which examined the impact of training on behaviour change, served as key resources for this study.

Although this approach provides a strong basis for the literature review, it is essential to recognize any potential constraints. These may entail partiality in selecting sources and shortages within existing research studies, specifically regarding the enduring effects of training and distinct modes of training.

2.4 Central Focus and Scope

The objective of this literature review is to comprehensively evaluate the influence of cybersecurity awareness training in healthcare environments, with a specific focus on its impact on medical project managers' practices and behaviours. Furthermore, it aims to assess how such training can reinforce security culture within healthcare organizations by examining various mechanisms that facilitate constructive behavioural changes among project managers while enhancing the overall level of protection against cyber threats. In addition, the study investigates different ways through which these trainings contribute towards fostering an environment characterized by heightened cybersecurity consciousness across all areas within health institutions. Lastly, effective strategies for gauging individual behaviour patterns as well as institutional outcomes concerning security indicators are identified so as to provide informative feedback. Ultimately, this research intends to offer insights into creating customized learning programs aimed at driving actual improvement and bolstering cyber safety measures throughout medical establishments.

2.5 Cybersecurity in Healthcare: Training & Foundations

The current landscape of cybersecurity awareness training in healthcare is marked by both progress and persistent challenges. While many healthcare organizations acknowledge the importance of such training and offer some form of program, the effectiveness and personalization of these efforts vary significantly (HIMSS, 2023). A notable gap exists in tailoring training materials to the specific responsibilities of medical project managers, hindering the application of knowledge to real-world scenarios (ISACA, 2023). It is crucial to implement training programs that specifically target the distinctive cybersecurity hazards inherent in healthcare project management. Figure 1 elucidates this necessity by outlining the escalating trends in healthcare cybersecurity such as telemedicine, AI and ML for threat detection and response, IoT connected medical devices, and regulatory compliance (BitLyft Cybersecurity).

Figure 1. Trends in Healthcare Cybersecurity

Source: The State of Healthcare Cybersecurity

2.6 Advancements and Obstacles

Cybersecurity awareness training in the healthcare industry has made significant progress lately. More and more healthcare organizations have adopted periodic employee training

programs, acknowledging that human factors are crucial in maintaining cybersecurity (Mireplex, 2023). A study conducted by KnowBe4 (2022) reveals that over 75% of healthcare workers received such coaching as of 2022. However, while this study highlights the increasing prevalence of training initiatives, it lacks insights into the specific content, quality, and effectiveness of these programs, leaving questions about their impact on actual behaviour change.

Nonetheless, there are still significant challenges to overcome. A 2022 study titled "The Need for Cybersecurity Training in Health Education Programs" found that only 18% of healthcare institutions offer yearly cybersecurity awareness training programs to their employees. This figure underscores an alarming disparity concerning the regularity and uniformity with which such initiatives take place.

A further hindrance exists in how training programs are structured and presented. Training that is generic and standardized often neglects to cater to the distinctive duties and obligations of various healthcare staff members. For instance, the cybersecurity requirements of a medical project manager differ greatly from those of a nurse or physician.

2.7 Need for Tailored Training Programs

Given the distinctive requirements of healthcare settings, it is imperative to design training modules that cater to the varied functions and duties within this industry. A generic approach is not suitable as each group necessitates customized instruction pertaining to their distinct needs; consequently, securing pertinent information delivered in an engaging format with achievable goals. Safa et al. (2016) examined the levels of information security awareness among healthcare professionals and observed that there were differences in understanding depending on factors like work position and background expertise. These outcomes underscore the significance of providing customized training initiatives targeting different requirements and knowledge gaps among various staff members within healthcare settings.

Medical project managers seek specialized training that emphasizes safeguarding project data, overseeing third-party vendors, and ensuring compliance with healthcare regulations. Conversely, nurses require instruction on upholding patient privacy, detecting phishing attacks, and properly utilizing medical equipment without compromising security.

2.7.1 Empirical Data and Case Studies

- **Case Study:** A 2023 study published in the Journal of Medical Internet Research found that merely 37% of hospitals carried out cybersecurity incident response exercises on an annual basis. This deficiency in hands-on training renders healthcare personnel ill-equipped to handle cyberattacks with any measure of competency. This highlights the gap between theoretical knowledge and practical application in cybersecurity training.
- **Empirical Data:** According to a report by Cybersecurity Ventures (2022), the healthcare sector is expected to invest more than $125 billion in cybersecurity products and services between 2020-2025, with an annual growth rate of around 15%. This indicates that there has been an increasing awareness among health organizations about the significance of securing their data. **However**, the same report also reveals that approximately 56% of companies spend less than 10 percent of their IT budget on cybersecurity. This suggests a potential disconnect between the recognized importance of cybersecurity and the actual allocation of resources to address it.

Concluding this section, the healthcare sector has made strides in cybersecurity awareness training; however, improvement is still paramount. Customized programs that keep pace with frequent updates and hands-on exercises are critical to empowering healthcare workers with proficiency for protecting sensitive patient data while combatting emerging cyber threats.

2.8 Theoretical Frameworks Underpinning Effective Training

Although there is no universal standard for cybersecurity, organizations can benefit from established guidelines and best practices outlined in Figure 2 to strengthen their security posture and training (Fortinet). Effective programs aimed at raising awareness about cybersecurity often rely on well-established theoretical frameworks that provide insights into human behaviour and motivation. These models serve as a foundation for understanding how individuals perceive risks, develop attitudes, and adopt secure behaviours; some of the key theories utilized in this context include:

- **Protection Motivation Theory (PMT):** According to this theoretical perspective, an individual is more likely to adopt protective behaviours when they perceive a threat as severe and believe they are susceptible to it. Consequently, training initiatives with palpable efficacy should underscore the gravity of cybersecurity vulnerabilities in healthcare settings while personalizing risk factors that relate directly to project managers' designated responsibilities (Johnston & Warkentin, 2010).
- **Social Cognitive Theory (SCT):** Social cognitive theory emphasizes the crucial role of observational learning and self-efficacy in facilitating desirable transformations in behaviour. To this end, training programs aimed at imparting best practices for project management ought to offer ample opportunities for professionals to observe secure behaviours being modelled while also affording them with a safe working environment that fosters confident practice sessions designed to bolster their ability to apply acquired skills effectively when confronted with challenging real-world scenarios (Compeau & Higgins, 1995).
- **Theory of Planned Behaviour (TPB):** According to TPB, intentions are the most significant predictors of behaviour. Therefore, training programs aimed at enhancing secure behaviours among project managers should prioritize addressing their attitudes towards security measures as well as perceived social pressure (subjective norms) and behavioural control perceptions (belief in their ability to perform the behaviour) (Ajzen, 1991). Although there is no universally recognized standards for cybersecurity, numerous establishments have opted to adopt particular guiding principles, precautions and technologies. Figure 2 illustrates a few of these examples.

Cybersecurity Management and Training Guidelines

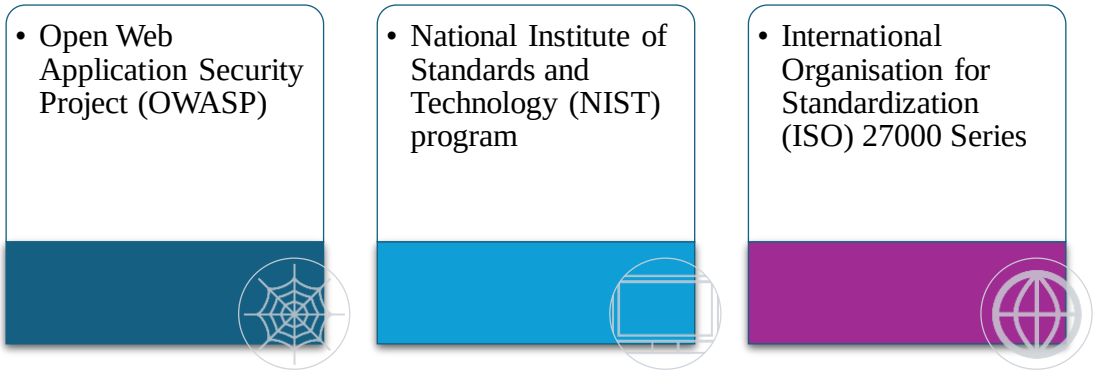


Figure 2. Cybersecurity Management and Training Guidelines

Source: Fortinet

2.9 Effective Training Design and Measurement in Healthcare Cybersecurity

Incorporating several key components is essential for medical project managers to receive effective cybersecurity awareness training. A case study was conducted by Shaw and Shiu (2020) to evaluate cybersecurity awareness training among healthcare organizations. Using a mixed-methods approach, they measured knowledge acquisition, behavioural changes, and organizational impact as indicators of the training's effectiveness. The resulting framework provides a holistic way of evaluating outcomes from such training. Components that are imperative include:

- **Tailored Content:** Training material must be tailored to cater to the exceptional cyber threats and difficulties that project managers encounter within healthcare environments. This may encompass topics such as evaluating risks, formulating security strategies, managing vendors, handling incidents, and complying with regulations like HIPAA.
- **Interactive Methods:** Utilization of interactive techniques like simulations, role-playing exercises, and quizzes can substantially improve engagement levels and knowledge retention compared to conventional passive learning methods (SANS Institute, 2023). According to a 2022 study by Alshehri et al. entitled "The Influence of Gamification on Cybersecurity Awareness and Conduct," gamified training resulted in substantial enhancements for participants' understanding of cybersecurity

as well as their self-assurance concerning the subject matter. The incorporation of such interactive elements can make training more engaging and effective for project managers.

- **Ongoing Reinforcement:** Constantly reinforcing cybersecurity awareness is crucial for establishing secure behaviours as habitual. This requires regular reminders, updates, and refresher training rather than relying on a one-time event to maintain vigilance (KnowBe4, 2023).

2.10 Measuring the Effectiveness of Training Programs

It is vital to assess the efficiency of cybersecurity awareness training for recognizing strengths, shortcomings, and opportunities for enhancement. Although pre- and post-training evaluations offer an understanding of knowledge acquired, they might not entirely reveal actual behavioural shifts (Kirkpatrick & Kirkpatrick, 2016). Thus, it is recommended to adopt a multi-faceted approach while evaluating that includes:

- **Behavioural Observation:** Improved practices resulting from training can be assessed by observing project managers' security behaviour in real-world situations. This provides a direct measure of whether the training has translated into tangible action.
- **Incident Reporting Analysis:** The examination of incident reports can yield valuable information regarding the occurrence and intensity of security incidents, both prior to and post-instruction. This data may suggest possible shifts in consciousness or conduct that have taken place due to training (ENISA, 2023). However, it's important to note that a decrease in reported incidents may not always directly correlate with improved security behaviour, as underreporting can also be a factor.
- **Qualitative Feedback:** Gathering qualitative feedback from participants through interviews or focus groups can provide valuable insights into their perceptions of the training and its impact on their work. This subjective data can complement quantitative measures and offer a deeper understanding of the training's effectiveness.

2.11 Challenges, Success Factors, and Research Gaps

2.11.1 Challenges and Barriers to Effective Training

Several challenges must be overcome to successfully implement and maintain cybersecurity awareness training for medical project managers. These include:

- **Time Constraints:** Project managers often face demanding schedules, making it difficult to allocate sufficient time for training. This challenge highlights the need for flexible and concise training formats that can be easily integrated into their workflow.
- **Limited Resources:** Due to resource constraints, healthcare organizations may not be able to create comprehensive training initiatives or employ dedicated cybersecurity experts. This underscores the importance of leveraging cost-effective training solutions and fostering collaboration with external partners.
- **Resistance to Change:** Some project managers may not perceive the value of cybersecurity awareness training or may resist altering their established practices. Addressing this challenge requires effective communication strategies that highlight the importance of cybersecurity and demonstrate the tangible benefits of training.

2.11.2 Success Factors and Best Practices

Despite the challenges, the literature identifies several key elements crucial for the success of cybersecurity awareness initiatives:

- **Leadership Support:** Strong leadership commitment is vital to ensure adequate resources, encourage participation, and cultivate a culture of security throughout the organization.
- **Tailored Content:** As highlighted by HIMSS (2023) and ISACA (2023), training material should be specifically tailored to the roles and responsibilities of medical project managers to ensure its relevance and applicability.
- **Interactive and Engaging Methods:** Research supports the use of interactive methods and gamification to improve engagement, knowledge retention, and behaviour change (Alshehri et al., 2022; SANS Institute, 2023).
- **Ongoing Reinforcement:** Continuous reinforcement through reminders, updates, and refresher courses is crucial for maintaining cybersecurity awareness and promoting long-term behavioural change (KnowBe4, 2023).

2.11.3 Research Gaps

Despite the valuable insights provided by existing literature, there remain substantial deficiencies in comprehending cybersecurity awareness training for medical project managers. These shortfalls consist of:

- **Long-term Impact:** While numerous studies focus on the immediate outcomes of training, there is a lack of research exploring the enduring effects on behaviour change and organizational security posture. Longitudinal studies are needed to understand how to sustain the benefits of training over time.
- **Impact of Specific Modalities:** Although interactive and engaging methods are recognized as effective, further research is necessary to evaluate the specific impact of modalities like gamification and microlearning on medical project managers.
- **Role of Organizational Culture:** The literature currently lacks a comprehensive understanding of how organizational culture influences the implementation and efficacy of training initiatives. Research is required to examine how cultural components impact the adoption of security practices and identify appropriate training interventions tailored to different corporate cultures.
- **Standardized Metrics:** The absence of uniform metrics to gauge the efficacy of training programs impedes comparisons between different organizations and their results. It is crucial to create comprehensive measures that evaluate both individual behavioural changes and organizational cybersecurity outcomes.

Addressing these research gaps will enhance our understanding of effective cybersecurity awareness training for medical project managers, contributing to improved security practices within the healthcare industry.

2.12 Conclusion

This literature review has emphasized the critical role of cybersecurity awareness training in influencing the behaviour of medical project managers and bolstering the overall security of healthcare institutions. While existing research demonstrates the positive impact of training programs on knowledge acquisition and attitude change, challenges persist in translating this knowledge into sustained behavioural modification and organizational security improvements.

2.12.1 Strengths of the Literature

The reviewed literature offers valuable insights into effective training practices, emphasizing the importance of tailored content, interactive methods, continuous reinforcement, leadership commitment, and robust evaluation frameworks. These elements provide a foundation for developing and implementing impactful cybersecurity awareness training programs.

2.12.2 Weaknesses and Research Gaps

Despite its strengths, the literature reveals gaps in understanding the long-term impact of training, the effectiveness of specific training modalities for medical project managers, the influence of organizational culture on training outcomes, and the need for standardized metrics to evaluate training effectiveness comprehensively.

Addressing these gaps will be crucial for advancing the field and developing more effective cybersecurity awareness training programs that empower medical project managers to protect sensitive patient data and contribute to a secure healthcare environment.

Chapter 3

Research Methodology

3.1 Introduction

An outline of the methodology, techniques and procedures employed to carry out this research is given in this chapter. The chapter is structured as follows: section 3.2 provides information on the research questions, 3.3 describes the research design used, while 3.4 highlights how data was collected and analysed using different approaches respectively; with implementation procedure detailed in Section 3.5, Ethical considerations, limitations encountered during the conduct of this study are discussed under sections 3.6, 3.7, finally conclusions drawn from findings obtained explained under section 3.8.

3.2 Research Questions

This research aims to explore the impact of project managers on cybersecurity in healthcare settings, by exploring the following queries:

1. How impactful are cybersecurity awareness training programs on medical project managers' conduct and the overall security posture of healthcare institutions?
2. How does cybersecurity awareness training specifically alter the conduct of medical project managers and enhance security practices within their projects?
3. Beyond individual behaviour change, how does training contribute to transforming the overall security culture within healthcare organizations?
4. What are the most effective methods for assessing the impact of cybersecurity awareness training on both individual behaviour and organizational security outcomes?

3.3 Study Design

For this study, a mixed-methods methodology was employed in this research, incorporating both qualitative and quantitative data gathering and analysis approaches. Quantitative information was obtained through surveys while interviews provided qualitative insights. The survey findings were analysed using descriptive statistics, whereas the interview responses were subjected to thematic investigation for pattern identification and theme extraction.

Figure 2 illustrates a flowchart that showcases the complete primary data collection process, including all stages ranging from preparation to finalization.

Primary Data Collection Flowchart

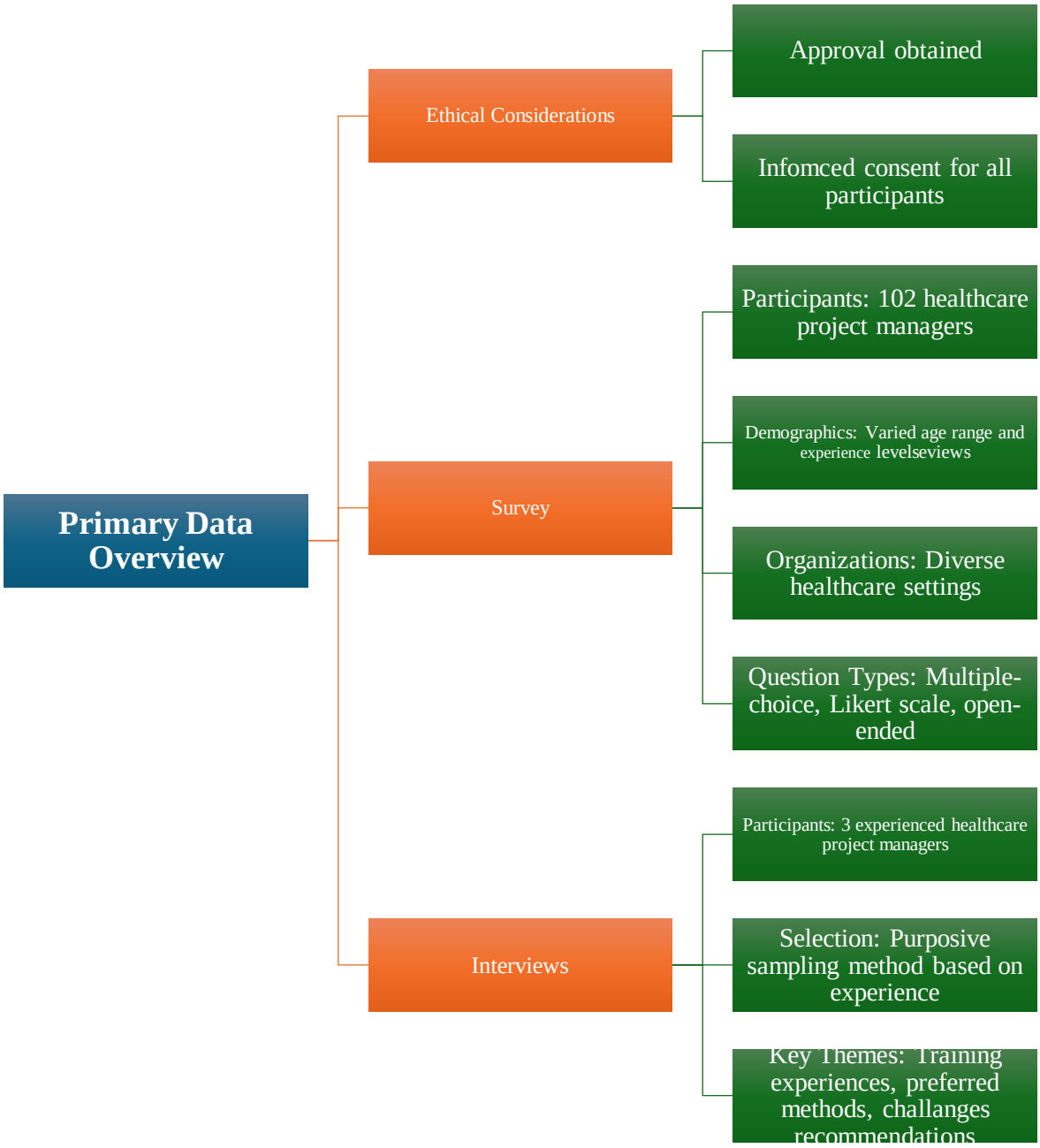


Figure 3. Primary Data Collection Flowchart

3.3 Methods of Data Collection

3.3.1 Sampling Methodology

To ensure that only survey participants with the necessary skills and experience were included, a purposive or judgment sampling method was utilized due to the specialized nature of project management and cybersecurity in healthcare.

3.3.2 Sample Size

To ensure a representative sample of project managers in healthcare organizations, the standard equation was utilized to determine the appropriate size for the sample.

3.3.3 Survey Administration and Data Collection

To gather extensive feedback from many participants, an online survey consisting of both close-ended (multiple-choice) questions was created. The questionnaire utilized a Informed Consent Form (ICF) and obtained respondents' consent before proceeding with the inquiry. Various channels were used for its distribution. This allowed for primary quantitative and qualitative data to be collected effectively.

3.3.4 Interview Administration and Data Collection

In addition to the survey, I engaged in individual interviews with professionals specializing in healthcare project management. By combining these two methodologies, we were able to acquire more comprehensive knowledge and support our discoveries through a versatile interview guide that allowed for flexibility and semi-structure.

3.4 Data Analysis Tools and Techniques

3.4.1 Quantitative Data Analysis

To examine and portray the findings obtained from the amassed data, several descriptive techniques such as mean calculations and percentage charts were employed. The analysis involved a range of factors like effectiveness of training programs and incidences related to cybersecurity.

3.4.2 Qualitative Data Analysis

The qualitative research data from interviews was analysed using thematic analysis. The study involved:

1. Familiarizing with the data by reading interview notes.
2. Generating initial codes to identify characteristics.
3. Searching for emerging themes.
4. Reviewing themes to ensure accuracy.
5. Defining and naming themes.
6. Summarizing and analysing data pertaining to the research questions.

3.4.2.1 Training Effectiveness Score (TES):

The equation evaluates the mean score indicating the effectiveness of training methods in modifying respondents' behaviour and retaining knowledge.

TES = (Σ (Effectiveness Rating * Number of Responses)) / Total Number of Responses

- **Effectiveness Rating:** Assign numerical values to each effectiveness level (e.g., Very Effective = 5, Effective = 4, etc.)
- **Number of Responses:** Count how many respondents chose each effectiveness level.
- **Total Number of Responses:** The total number of respondents who answered the question about effectiveness.

3.4.2.2 Training Relevance Score (TRS):

The equation determines a mean score that reflects the perceived applicability of the training content to participants' distinct job responsibilities.

TRS = (Σ (Rating * Number of Responses)) / Total Number of Responses

- **Rating:** Assign numerical values to each relevance level (e.g., Very relevant = 5, Somewhat relevant = 4, etc.)
- **Number of Responses:** Count how many respondents chose each relevance level.
- **Total Number of Responses:** The total number of respondents who answered the question about relevance.

3.5 Implementation Process

3.5.1 Preparation

The survey was created and shared on the internet, while its link spread through professional networks. During interviews, pertinent associations were formally asked for participation and ICF provided volunteers with comprehensive details.

3.5.2 Survey Administration

Before participating in the survey, volunteers were assessed to determine their suitability. The survey was only completed by those who met the screening criteria and provided consent. By GDPR guidelines, privacy measures were implemented to protect participants' information.

3.5.3 Conducting Interviews

Individuals interested in participating volunteered via professional associations and networks. Afterwards, a formal request with detailed information about the research was sent to each volunteer by the ICF team so that they could make an informed decision about whether to participate in virtual interviews. Those who agree and give their consent are then interviewed willingly as participants of the study.

Before the main interview questions, screening and eligibility determination were conducted through leading questions. Those deemed eligible were then given a chance to share their experiences-based opinions using open-ended queries that occasionally led into follow-up inquiries for capturing more information. Due to healthcare and employment roles' sensitivity, recording was generally refused; hence detailed notes provided points of reference for clarifications later. In total, three participants partook in the main interview process.

3.6 Ethical Considerations

Ethics approval was obtained prior to data collection. The ICF provided detailed information to participants, who participated voluntarily and gave consent. Both the survey and interviews were anonymized, and data was kept confidential.

3.7 Limitations of the Study

It is important to consider the limitations of this study when interpreting its results. While purposive sampling was used, it may not provide a complete representation of healthcare

project managers as a whole and therefore could constrain the applicability of findings. Moreover, relying solely on self-reported data obtained from surveys or interviews can introduce inaccuracies into the research since participants might exaggerate their understanding of cybersecurity issues or withhold details regarding security incidents they have experienced.

In addition, the limited focus of the study on project managers fails to encompass all the cybersecurity challenges that healthcare organizations face. This neglects other important stakeholders and their viewpoints. Nonetheless, utilizing a mixed-methods approach strengthens this research by providing both quantitative and qualitative perspectives. Future studies with a broader range of participants and data sources could confirm or broaden these findings even more significantly.

3.8 Conclusion

The mixed-methods approach incorporates both qualitative and quantitative data to offer a well-rounded perspective of healthcare project management and cybersecurity. By utilizing surveys, we obtained insight into the frequency and categories of cyber threats that are foremost in the minds of healthcare project managers, as well their understanding levels regarding current practices. The integration of semi-structured interviews enabled deeper exploration into how various individuals navigate through unique experiences when implementing security measures for their projects within this industry's parameters.

The all-encompassing approach of this methodology facilitates a comprehensive comprehension of the cybersecurity spectrum in healthcare project management, while also revealing the subtleties and contextual factors that impact its success. This study integrates empirical data with detailed qualitative accounts to produce practical guidance customized for the unique requirements and limitations faced by healthcare project managers, making a noteworthy contribution towards creating a secure environment within healthcare realms.

Chapter 4

Results, Analysis, and Implications

4.1 Introduction

The current chapter delves into a thorough analysis and interpretation of the research findings. To synthesize these insights, both quantitative data obtained from surveys and qualitative perspectives derived from interviews are utilized. The study involved 102 participants who responded to our inquiries through surveys, as well as three healthcare project management professionals with whom we conducted interviews. These sources serve to address the four primary research questions that have guided this investigation:

1. How impactful are cybersecurity awareness training programs on medical project managers' conduct and the overall security posture of healthcare institutions?
2. How does cybersecurity awareness training specifically alter the conduct of medical project managers and enhance security practices within their projects?
3. Beyond individual behaviour change, how does training contribute to transforming the overall security culture within healthcare organizations?
4. What are the most effective methods for assessing the impact of cybersecurity awareness training on both individual behaviour and organizational security outcomes?

The chapter is structured as follows:

- Section 4.2 comprehensively explores the survey results by examining the responses to every question in detail and draws out their implications for addressing the research questions.
- Section 4.3 emphasizes the qualitative findings obtained from conducting interviews, highlighting significant themes and trends that surfaced during the conversations.
- Section 4.4 merges the results obtained through surveys and interviews, emphasizing similarities as well as differences. This provides a holistic viewpoint on the research inquiries.

- Section 4.5 concludes the chapter by summarizing the main takeaways and their significance for cybersecurity practices within healthcare project management.

This chapter's objective is to offer a comprehensive understanding of the intricate relationship between cybersecurity, project management, and healthcare industry challenges by merging both quantitative and qualitative data. Specifically, we will delve into topics such as the prevailing state of cybersecurity training awareness within organizations concerning its influence on project manager practices and organizational security while simultaneously highlighting areas where improvements can be made.

4.2 Detailed Survey Analysis and Implications

4.2.1 Job Titles (Q1)

- **Results:** All the respondents (100%) identified as Healthcare Project/Product Managers, confirming the survey's focus on this target group.

- **Implications:** The substantial presence of project managers guarantees that the results are pertinent to comprehending their requirements for cybersecurity awareness and instruction.

- **Connection to Research Questions:** This discovery pertains to the initial research query concerning how cybersecurity awareness training affects various positions in healthcare institutions. It emphasizes the significance of customizing training regimes according to project managers' specific duties and difficulties.

4.2.2 Years of Experience in Current Role (Q2)

- **Results:** The survey revealed that a significant majority of respondents (over 80%) possess substantial experience in their current roles within healthcare organizations. The distribution is as follows:

    a) Less than 1 year: 2.38%
    b) 1-3 years: 23.81%
    c) 4-6 years: 35.71%
    d) 7-10 years: 28.57%
    e) More than 10 years: 19.05%

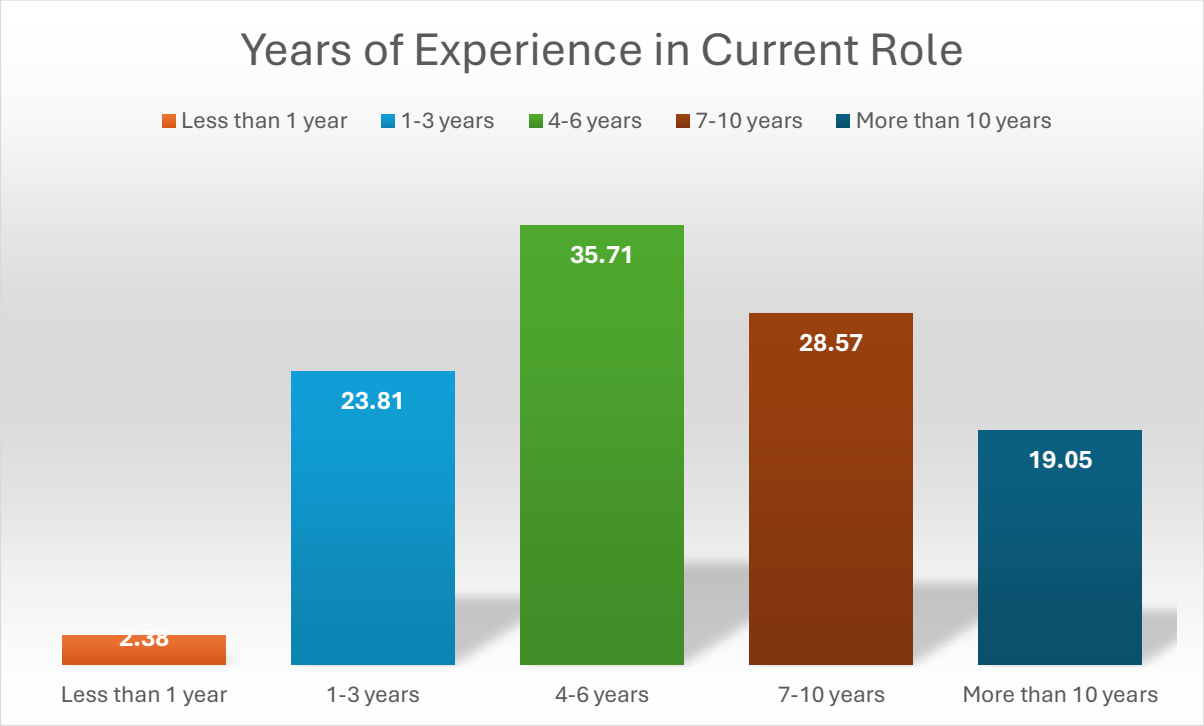


Figure 4. Years of Experience

- **Implications:** The survey encompassed the viewpoints of proficient healthcare project managers, as evidenced by many respondents possessing 4+ years of experience. This expertise fosters an enhanced awareness regarding cybersecurity hazards and emphasizes effective training initiatives to mitigate these risks. Furthermore, even individuals with under three years of practice contributed

meaningful perspectives towards identifying onboarding and instructional requirements for novice healthcare project managers.

- **Connection to Research Questions:** This discovery holds relevance to the fundamental inquiry of how cybersecurity awareness training affects the conduct and safeguarding methodologies of medical project managers. It could be postulated that individuals with greater expertise may possess distinct training requirements and anticipations in comparison to those who are freshers in this sector. Further, these findings can aid in evaluating whether proficiency level is linked to self-assurance when dealing with cyber-security incidents or attitudes towards security culture within an organization.

4.2.3 Type of Healthcare Organization (Q3)

- **Results:** A wide array of healthcare settings were included in the survey, revealing valuable information about different organizations' distinct cybersecurity concerns and focal points. The breakdown is as follows:

a) Hospital: 30.95%
b) Clinic: 7.14%
c) Long-term care facility: 28.57%
d) Medical Laboratory: 14.29%
e) Other: 19.05%

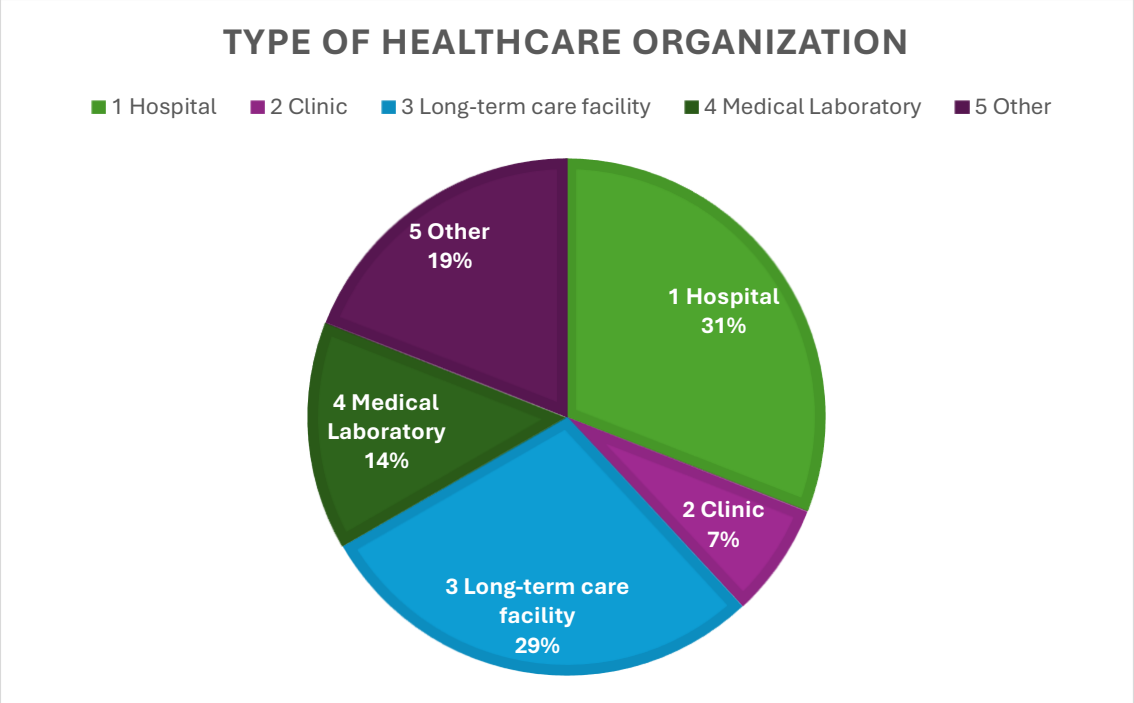


Figure 5. Type of Healthcare Organization

- **Implications:** The study's results are widely applicable to a range of healthcare settings, including hospitals, clinics, and long-term care facilities. Each setting presents unique cybersecurity challenges: hospital IT infrastructures and sensitive patient data may be at greater risk for cyberattacks; in contrast, protecting vulnerable populations' privacy is an area of concern for long-term care facilities. Understanding these distinctions allows tailored training programs for project managers across different environments. Furthermore, the "Other" category includes various institutions such as research organizations or pharmaceutical companies that expand the scope beyond traditional healthcare providers. These findings suggest implications extending far beyond typical healthcare contexts.

- **Connection to Research Questions:** The presented data is vital in the investigation of cybersecurity-related inquiries, as it furnishes a framework for comprehending how healthcare institutions' awareness and training requirements may fluctuate. It emphasizes the significance of considering individual hurdles and preferences when creating or instituting preparation modules while perhaps illuminating disparities

concerning perceived effectiveness towards education initiatives alongside adopting cyber defence best practices among different organizational categories.

4.2.4 Direct Responsibility for Managing Electronic Health Records (EHR) Systems (Q4)

- **Results:** A striking 90.48% of survey participants affirmed that their role involves direct responsibility for managing Electronic Health Records (EHR) systems, whether directly or indirectly.

- **Implications:** The dominant majority highlights the vital role that EHR systems play in the daily operations of healthcare project managers. These digital depositories contain sensitive patient data, making them attractive targets for cyberattacks. The fact that almost all survey participants have a direct involvement in managing these systems reiterates the urgent need for robust cybersecurity knowledge and skills within this profession. Decisions made by these professionals can directly affect how secure patient information remains regarding confidentiality, integrity, and availability. Even those who don't manage EHRs (comprising only 9.52%) may still interact or participate in relevant projects impacting system security - hence their opinions are valuable when understanding broader cybersecurity issues affecting healthcare institutions.

- **Connection to Research Questions:** This discovery pertains directly to several fundamental research inquiries. It emphasizes the potential influence that cybersecurity education can have on the actions and methods of project managers who hold direct accountability for protecting confidential patient information. Furthermore, it stresses how indispensable training initiatives are in addressing specific EHR system-related vulnerabilities and challenges regarding cybersecurity.

4.2.5 Cybersecurity Awareness Training in the Past Year (Q5)

- **Results:** According to the survey, most respondents (90.48%) had undergone cybersecurity awareness training in the previous year while only a few (9.52%) reported not receiving any form of such training during that duration.

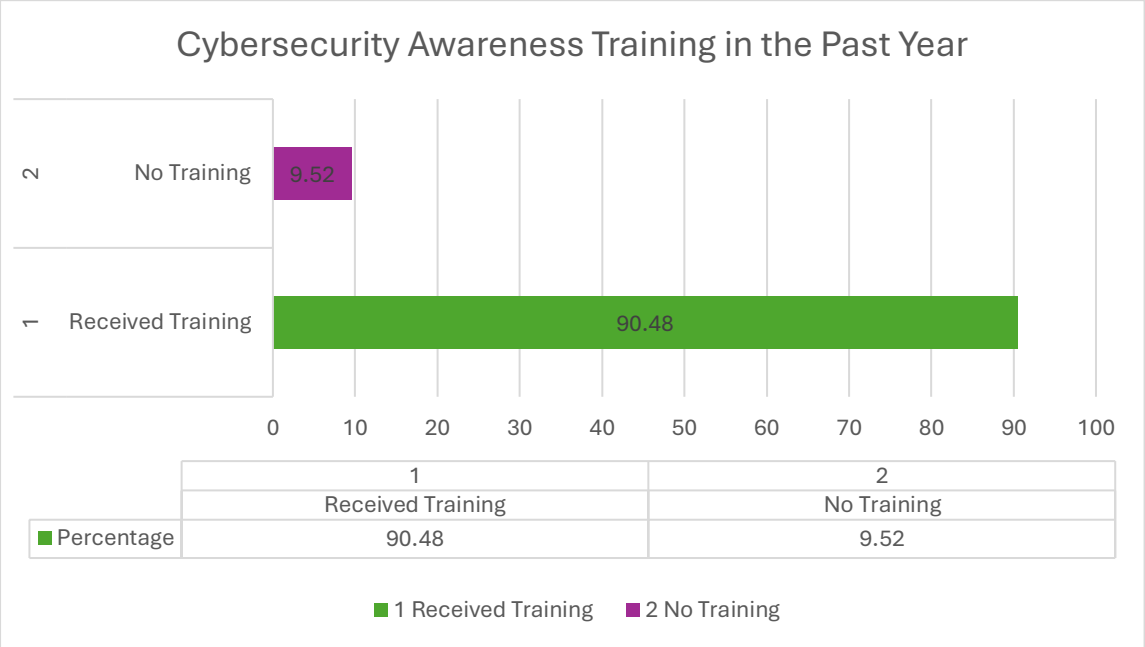


Figure 6. Cybersecurity Awareness Training in the Past Year

- **Implications:** An increasing number of healthcare organizations acknowledge the significance of cybersecurity awareness, as reflected by a sizeable proportion of respondents who received training. This denotes favourable progress towards arming project managers with the competence to tackle cyber threats proactively. Nevertheless, it is alarming that roughly 10% of participants were not trained and indicates potential inadequacies in coverage for job functions or specific firms. It emphasizes persisting endeavours to guarantee that all healthcare project managers receive access to and engage in cybersecurity education courses.

- **Connection to Research Questions:** The presented discovery has a direct connection to the fundamental inquiry on cybersecurity awareness training impact. It establishes a basic comprehension of the present training status among healthcare project

managers. Further scrutiny can investigate how participation in such programs relates to diverse outcomes, including modifications in work approaches, increased confidence while handling incidents and viewpoints on organizational security culture.

4.2.6 Frequency of Organizational Cybersecurity Training (Q6)

- **Results:** The survey revealed varying frequencies of cybersecurity training across healthcare organizations:

a) Quarterly: 54.76%
b) Annually: 26.19%
c) Monthly: 16.67%
d) Never: 2.38%

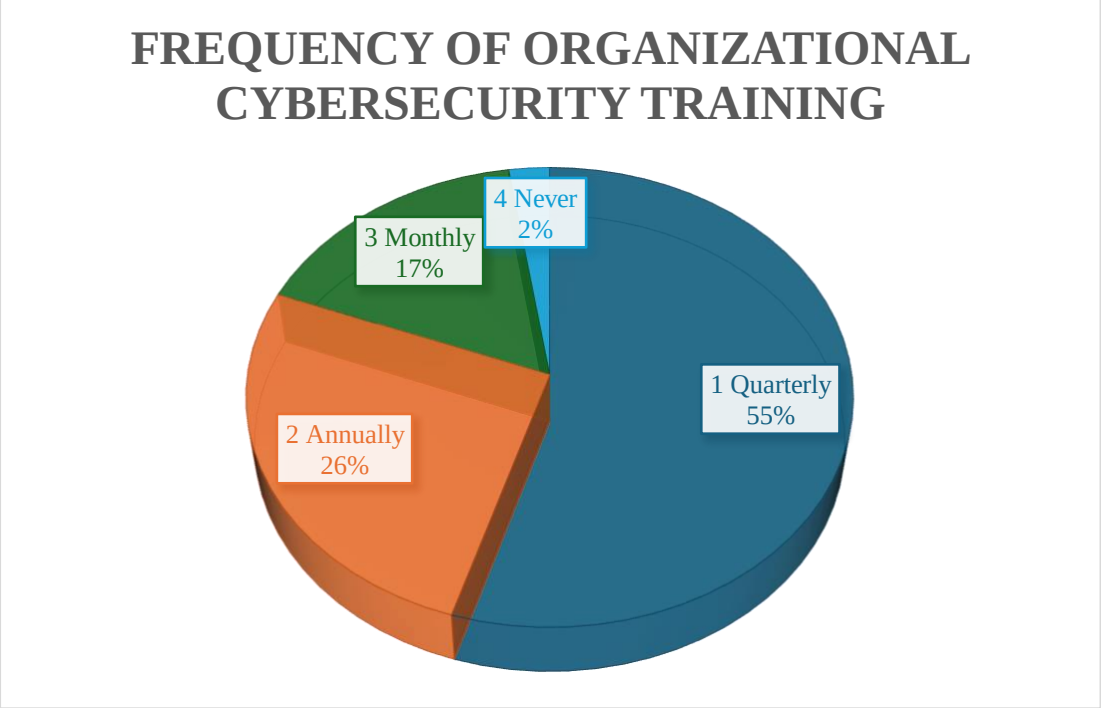


Figure 7. Frequency of Organizational Cybersecurity Training

- **Implications:** Many organizations take a proactive approach to keeping their staff updated on evolving threats and best practices by providing cybersecurity training

quarterly. However, there is room for improvement as over 25% of respondents receive annual training only, while some even get no training at all which is concerning. The dynamic nature of cyber threats requires ongoing education and reinforcement to maintain a strong security posture, particularly in the healthcare sector.

- **Connection to Research Questions:** There is a direct connection to the research queries that delve into how cybersecurity awareness training impacts healthcare and the difficulties experienced when implementing it. It prompts one to ponder on what frequency of training would be optimal for project managers within the field, as well as whether more frequent courses translate to better security outcomes. Furthermore, it emphasizes the importance of overcoming barriers limiting access to such training while simultaneously encouraging an ongoing culture dedicated to learning all things related to cybersecurity.

4.2.7 Relevance of Training Content to Specific Role (Q7)

- **Results:** The survey indicated a strong positive perception of the relevance of cybersecurity training content to the respondents' roles, with:

    a) Very relevant: 73.81%
    b) Somewhat relevant: 23.81%
    c) Neutral: 2.38%
    d) Somewhat irrelevant: 0%
    e) Very irrelevant: 0%

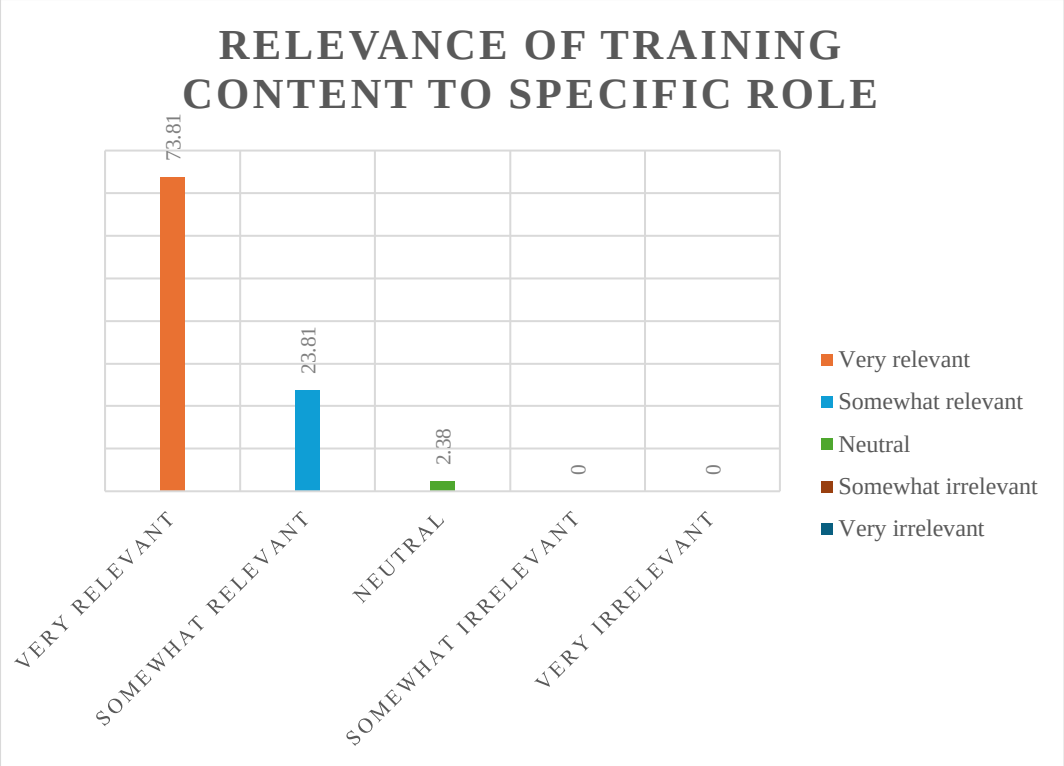


Figure 8. Relevance of Training Content to Specific Role

- **Implications:** The survey results indicate that the training content is well-matched with healthcare project managers' needs and expectations, as evidenced by 97.62% of respondents rating it "very relevant" or "somewhat relevant." Maintaining alignment in this area is essential because irrelevant materials can cause disinterest and hinder learning effectiveness. The lack of unfavourable ratings further supports the general suitability of the program's resources. However, responses classified as "neutral" reveal a need to enhance customization for distinct roles within healthcare project management so they better fit individual responsibilities.

- **Connection to Research Questions:** This addresses inquiries into the influence and efficiency of cybersecurity awareness education, emphasizing the significance of supplying fitting and customized material that appeals to healthcare managers' particular necessities. The substantial relevance score signifies that present training initiatives are mostly effective in meeting this aim. However, there's an opportunity to

enhance them further for optimal involvement and knowledge dissemination purposes.

4.2.8 Topics Covered in Most Recent Cybersecurity Training (Q8)

- **Results**: The survey allowed participants to select multiple topics covered in their most recent cybersecurity training. The results highlight the areas emphasized in current training programs:

a. Risk assessment and management: 80.95%
b. Protecting sensitive patient data: 76.19%
c. Regulatory compliance (e.g., HIPAA, GDPR): 64.29%
d. Secure use of medical devices and equipment: 54.76%
e. Phishing and social engineering: 47.62%
f. Incident response planning: 35.71%
g. Vendor management: 28.57%
h. Other: 0.00%

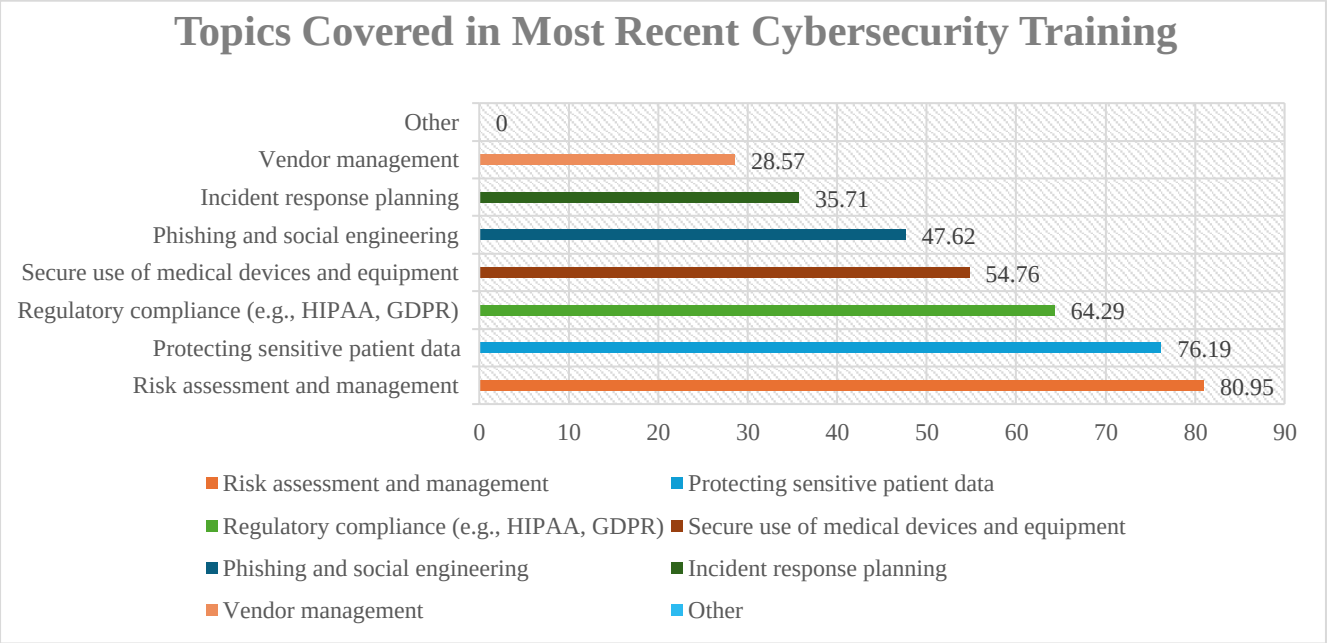


Figure 9. Topics Covered in Most Recent Cybersecurity Training

- **Implications**: The significant figures for "risk assessment and management" as well as "protecting sensitive patient data" illustrate how crucial they are in healthcare cybersecurity training. This highlights not only their importance but also the urgent need to safeguard confidential information while reducing potential risks. The emphasis on regulatory compliance further emphasizes the significance of adhering to relevant laws and standards, underscoring its critical role for project managers. Additionally, incorporating topics such as phishing, secure device usage, and incident response planning indicates a strong focus on addressing common vulnerabilities that pose threats to this field's overall security measures. However, due to healthcare IT heavily relying upon third-party vendors' services or products; it suggests a lower percentage for vendor management implying an area where more attention could be dedicated to future training programs intending greater scrutiny over these external resources involved with healthcare practices. It is suggested more concentration should entail this aspect since it has rising implications concerning electronic medical records (EMRs).

- **Connection to Research Questions**: The results of the study specifically pertain to investigating cybersecurity awareness training's content and effectiveness as they relate to healthcare project managers. These findings shed light on focus areas in current programs, and their alignment with perceived needs, and can reveal gaps in coverage that could inform more thorough and specific program development efforts.

4.2.9 Training Methods Used (Q9)

- **Results**: The survey allowed participants to select multiple training methods used in their most recent cybersecurity awareness programs. The results showcase the diversity of approaches employed:

    a) Online module/eLearning: 78.57%
    b) In-person workshops or seminars: 69.05%
    c) Quizzes/Assessments: 52.38%
    d) Simulations/Role-playing exercises: 42.86%

e) Gamified training elements: 26.19%

f) Other: 0.00%

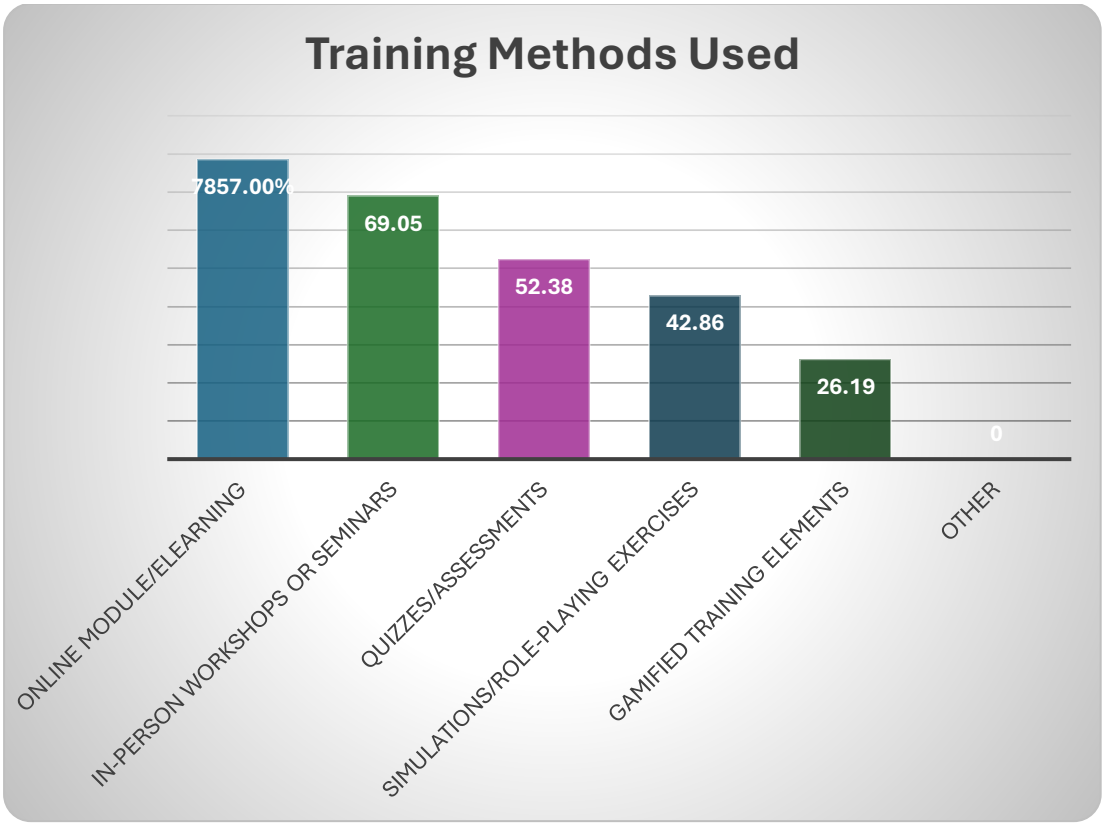


Figure 10. Training Methods Used

- **Implications**: Healthcare cybersecurity training is starting to incorporate more engaging and interactive techniques. A blended learning approach appears to be the preferred method for healthcare cybersecurity training, given the widespread use of both online modules/eLearning and in-person workshops. Online modules offer convenience while in-person workshops provide chances for collaboration. The emphasis on quizzes/assessments shows a need to evaluate learning outcomes effectively, whereas including simulations/role-play exercises implies an increased recognition of experiential learning's value. Although gamified elements are infrequent, their presence hints at incorporating captivating approaches into healthcare

cybersecurity training program design. an increasing interest in using engaging and interactive methods to enhance learning.

- **Connection to Research Questions**: Results of this question are relevant to the study into which cybersecurity training methods yield superior outcomes. They shed light on prevailing practices in healthcare and their potential influence on knowledge retention, behavioural modification, and overall efficacy of training.

4.2.10 Perceived Effectiveness of Training Methods (Q10)

- **Results**: Question 10 in the survey employed a slider scale that spanned from 0 to 100. This scale enabled participants to assess how effective they found the training methods for aiding retention of information and inducing behavioural change.

    - Most responses clustered between 60 and 80, signifying a generally positive perception of training efficacy.
    - However, a notable distribution towards lower ratings was also observed, indicating varying opinions on training impact.
    - The most frequent response appeared around 75, suggesting an overall favourable view of training effectiveness.

- **Implications**: The variety of reactions illustrates the intricacy involved in gauging training efficacy, emphasizing how crucial it is to account for individual disparities linked with learning styles, previous knowledge, and ambition. Although a generally optimistic outlook is heartening, lower scores reveal crucial facets that require enhancement. The results suggest some techniques might not wield universal success; hence, more investigation should identify elements that enhance or impede memorization as well as influence behavioural adjustments.

- **Connection to Research Questions**: Findings are directly connected with the fundamental research question concerning cybersecurity awareness training's influence on conduct and healthcare organizations' overall security stance. It offers valuable viewpoints into different training techniques' perceived effectiveness, which can assist in designing and executing upcoming programs. Furthermore, it highlights the necessity of going beyond just gauging knowledge acquisition to evaluate actual behavioural changes and their effect on organizational safety measures.

4.2.11 Changes in Work Practices due to Cybersecurity Training (Q11)

- **Results**: The survey asked if the participants had altered any of their work practices as a result of cybersecurity training, and the results indicated that most acknowledged making beneficial changes in behaviour:

    - Yes: 85.71%
    - No: 14.29%

- **Implications**: Cybersecurity training has proven to be effective in prompting changes among a significant proportion (85.71%) of respondents, indicating its success in translating knowledge into action and empowering healthcare project managers to enhance their organization's cybersecurity practices. However, the remaining 14.29% who reported no change serve as a reminder that achieving consistent and sustainable behavioural modification through training remains an ongoing challenge, highlighting the need for understanding potential obstacles and developing appropriate strategies for overcoming them.

- **Connection to Research Questions:** The question pertains to the central research questions concerning how cybersecurity awareness training affects behaviour and organizational security. It presents convincing proof that undergoing such a program can foster desirable alterations in work-related practices, thereby bolstering healthcare organizations' overall security posture.

4.2.12 Changes in Work Practices Due to Cybersecurity Training (Q12)

- **Results**: The question provided an opportunity for the respondents to detail their work practice modifications after receiving cybersecurity training. Alternatively, they could offer reasons for failing to make any meaningful changes. A scrutiny of the feedback showed that there was a varied assortment of measures taken alongside obstacles encountered in implementing them.

    - *Positive Changes**:*** The majority of those surveyed stated that they have become more vigilant in their actions, such as carefully examining email origins and staying away from dubious downloads. This indicates an increased understanding of phishing and social engineering tactics. Additionally, many mentioned incorporating advanced measures for securing data and improving network security to take pre-emptive steps towards protecting confidential patient information. Some interviewees even commented on the benefits gained through training programs which helped enhance their comprehension about cybersecurity issues as well as boost overall confidence in dealing with them effectively.

    - *Barriers to Change**:*** Several surveyed individuals mentioned the idea that their current methods were satisfactory, highlighting a potential difficulty in inspiring those who do not recognize an urgent requirement for modification. Meanwhile, certain people cited limited resources and implementation obstacles as hindrances to embracing fresh security measures. Only a minuscule percentage of respondents noted no need for alteration,

underscoring the significance of determining and exhibiting the relevance and pressing nature of cybersecurity training.

- **Implications**: The complexity of factors affecting behaviour change in cybersecurity training is exemplified by the wide array of responses to this question. Although there were generally favourable reports, barriers that emerged revealed the importance for organizations to furnish ample resources and support while also encouraging motivation to achieve success with implementing new security practices. Valuable insights into specific actions taken by project managers and obstacles encountered were gleaned from open-ended feedback which can guide improvements in developing more effective training programs and strategies for managing changes.

- **Connection to Research Questions**: The results specifically tackle the research question of how cybersecurity awareness training affects behavioural modifications. The answers showcase tangible instances where such instruction could facilitate the adoption of fresh safety techniques, indicating its ability to lift healthcare establishments' overall security stance. Further, the obstacles outlined expose difficulties related to converting know-how into action and serve as useful pointers for boosting instructional efficacy while encouraging perpetual changes in conduct patterns.

4.2.13 Confidence in Handling a Cybersecurity Incident (Q13)

- **Results:** Respondents' confidence in their ability to handle a cybersecurity incident in their role was evaluated using Survey Question 13, which utilized a slider scale ranging from 0-100
    - Most responses fell between 70 and 90, indicating a substantial number feel reasonably confident.
    - There was also a spread towards lower ratings, suggesting some individuals feel less prepared.

- The most frequent response was around 75, indicating a generally positive but not overly confident perception.

- **Implications:** The findings indicate that healthcare project managers have varying levels of confidence in their capacity to respond to cybersecurity incidents. Although a majority reported moderate to high self-assurance, the existence of lower scores emphasizes the requirement for more training and assistance in bolstering preparedness. The variability in assurance might relate to factors such as experience, received instruction, and support from organizations.

- **Connection to Research Questions:** This finding has a direct correlation with the research questions that delve into how cybersecurity awareness training affects behaviour and the overall security stance of healthcare institutions. It sheds light on project managers' perceived self-efficacy in coping with cyber-attacks, which holds sway over their actions and judgment during crises. Additionally, it highlights the value of educational schemes that not only equip learners but also boost their confidence to respond proactively.

4.2.14 Promotion of Cybersecurity Awareness Culture within the Organization (Q14)

- **Results:** Respondents' perception of their organization's promotion of cybersecurity awareness culture was measured using a slider scale ranging from 0 to 100 in Survey Question 14

  .

  - The distribution of responses was skewed towards the lower end of the scale, with a noticeable peak at 0-10.
  - This suggests that most participants perceive their organizations as having minimal prioritization of cybersecurity awareness.

- While there was an upward trend towards the middle of the scale (around 50-60), the overall results indicate significant room for improvement.

- **Implications**: Concerns are raised by the findings regarding cybersecurity culture in numerous healthcare organizations. A deficiency of emphasis on awareness towards cybersecurity can lead to vulnerabilities and escalate the probability of accomplished cyberattacks. The ratings being low indicate that several project managers do not perceive their organizations actively encouraging a sense of collective security responsibility, which may result in complacency and inadequate vigilance further enabling cybercriminals to exploit weaknesses. Thus, it is imperative for healthcare institutions prioritizing developing resilient cybersecurity cultures based on these outcomes.

- **Connection to Research Questions**: Results are directly associated with the research inquiries that investigate how training influences the security status of healthcare establishments. It implies that despite having efficient training schemes, a deficient organizational culture can impede the implementing secure methods and diminish cybersecurity effectiveness significantly.

4.2.15 Challenges in Attending or Benefiting from Cybersecurity Training (Q15)

- **Results**: Respondents were presented with a multiple-choice question to identify the primary obstacles they encounter when participating in or benefiting from cybersecurity training. The findings reveal notable impediments as follows:

1. Time constraints: 66.67%
2. Difficulty applying knowledge to real-world scenarios: 47.62%
3. Insufficient resources dedicated to training: 38.10%
4. Lack of relevant training material to my role: 33.33%

5. Lack of interest/awareness in the topic: 23.81%
6. Other: 0.00%

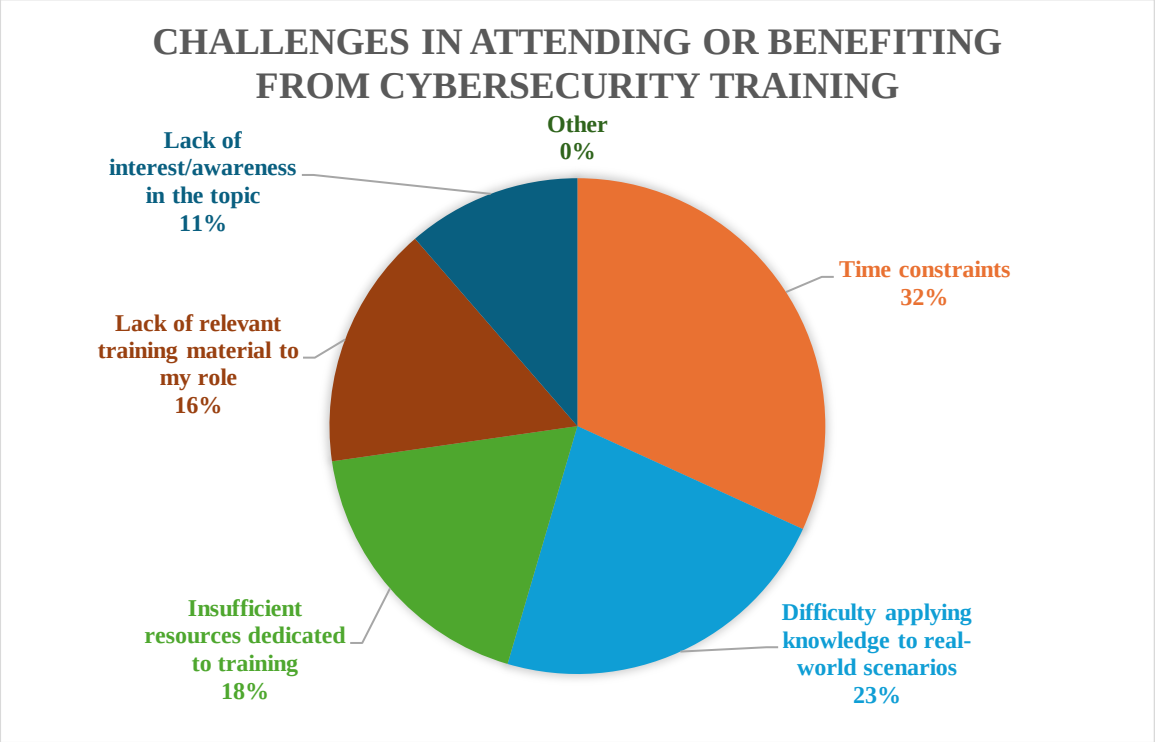


Figure 11. Challenges in Attending or Benefiting from Cybersecurity Training

- **Implications:** The fact that "time constraints" are a significant challenge emphasizes how demanding healthcare project management roles can be and the difficulty in juggling training with other responsibilities. Most respondents reported struggling to apply their knowledge in practical situations, emphasizing the necessity for more hands-on training methods. Concerns regarding inadequate resources and insufficient role-specific learning materials suggest potential deficiencies in organizational aid towards cybersecurity education investments.

- **Connection to Research Questions**: The results directly correlate to the research objectives that examine obstacles faced while implementing efficient cybersecurity training and its influence on behavioural alteration. They expose significant hurdles

that medical institutions must overcome to guarantee project managers' complete involvement in instruction programs. Additionally, they emphasize the necessity for practical, current, and captivating content in these courses to enable project directors to effectively apply their knowledge towards real-life scenarios; thus, contributing towards a firmer security mechanism.

4.2.16 Recommendations for Improvement in Cybersecurity Awareness Training (Q16)

- **Results:** In Survey Question 16, the participants were asked to provide suggestions on how their organizations could enhance cybersecurity awareness training. They had the option of choosing more than one recommendation. The resulting key priorities are as follows:

1. More interactive and engaging training methods: 64.29%
2. More frequent training sessions: 61.90%
3. More opportunities to practice skills in a safe environment: 59.52%
4. Stronger leadership support and messaging: 57.14%
5. Continuous reinforcement and updates: 50.00%
6. More tailored content for specific roles: 45.24%

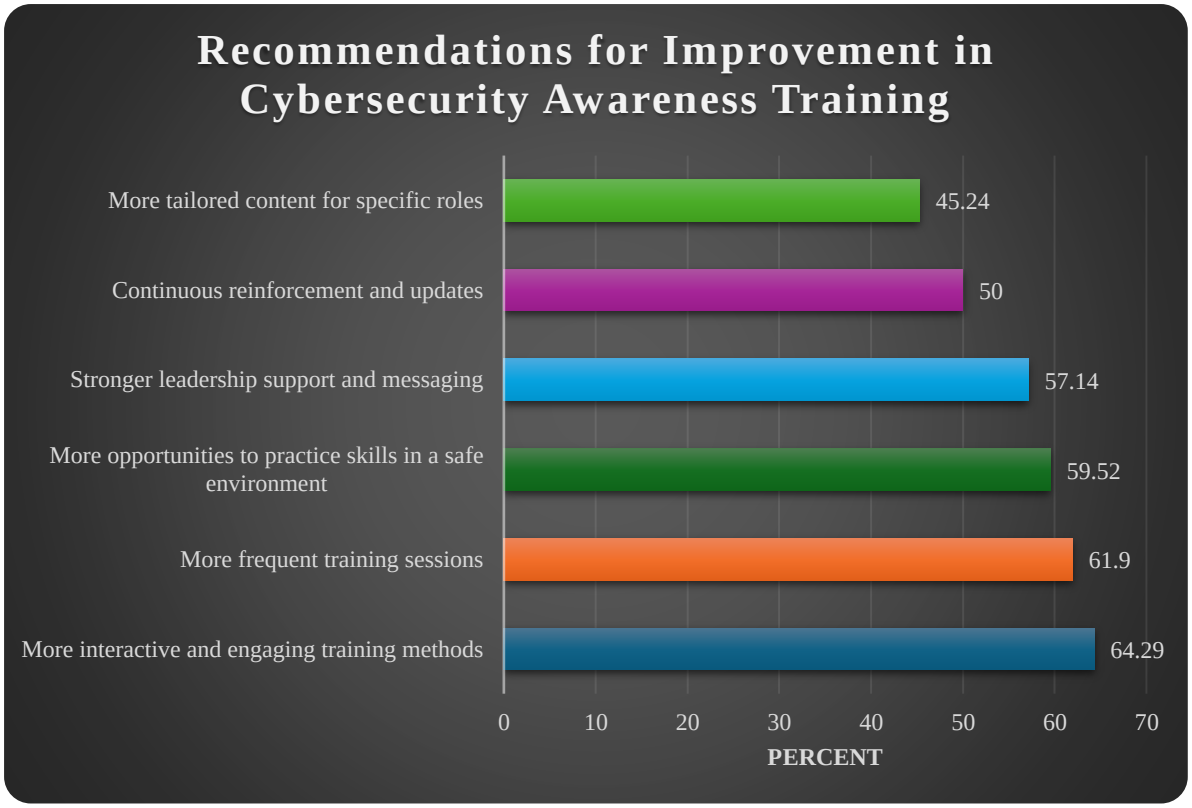


Figure 12. Recommendations for Improvement in Cybersecurity Awareness Training

- **Implications**: The prevalence of interactive and engaging training methods highlights the inadequacy of traditional, passive approaches to cybersecurity education in captivating healthcare project managers. The frequency desired for training sessions acknowledges that continuous reinforcement is necessary to maintain effective cybersecurity awareness amid ever-evolving threats. Emphasizing on experiential learning and gaining confidence through applying knowledge underscores the significance of practising skills in a secure environment. Stronger leadership support and messaging demonstrate organizational leaders' critical role in cultivating a culture centred around cybersecurity awareness while demanding more personalized content emphasising the importance of recognizing individual roles within healthcare organizations by providing relevant actionable training tailored towards them.

- **Connection to Research Questions:** The recommendations presented specifically tackle the research questions investigating barriers to and possibilities for enhancing

cybersecurity training efficacy. They furnish practical ideas on how to upgrade current training programs and foster a security-driven mindset across healthcare establishments. The results stress the importance of employing diverse techniques, consistent reinforcement, leadership backing, and customized content in creating a powerful cybersecurity training program that yields favourable outcomes.

4.2.17 Additional Comments and Suggestions (Q17)

Question 17 of the survey created an opportunity for participants to freely express their valuable perspectives and suggestions regarding cybersecurity awareness training specifically targeted towards project managers in healthcare. The qualitative data obtained from this question is highly significant as it provides diverse insights that go beyond the predetermined responses collected from earlier questions.

4.3 Key Themes

The analysis of these comments highlighted a strong emphasis on the following aspects:

1. **Continuous and Frequent Training:** Participants emphasized the importance of continuous and frequent cybersecurity instruction, rather than isolated occasions. This indicates a recognition that cyber threats are constantly changing and evolving, necessitating project managers to remain informed about emerging dangers and optimal protocols.

2. **Tailored and Relevant Content:** Several participants stressed the importance of tailored training catered to healthcare project managers' duties and obligations. This underscores the value of imparting pragmatic and implementable expertise that directly relates to their job functions.

3. **Interactive and Engaging Methods:** According to the respondents, they prefer interactive training formats like simulations and real-world scenarios. This shows that

they want immersive learning experiences where they can actively participate and use their knowledge in practical situations.

4. **Leadership Support and Communication:** Clear communication and strong leadership support from the top were highlighted as essential in fostering a culture of cybersecurity awareness throughout the organization.

Additional Suggestions

Other notable suggestions from respondents included:

1. Ensuring training is easily understandable and available to all employees, regardless of their technical knowledge.

2. Real-life scenarios and instances should be used to demonstrate the significance of cybersecurity breaches.

3. Sending frequent messages or reminders daily to strengthen important ideas.

4.4 Cybersecurity Awareness Training in Healthcare: Project Manager Perspectives

In this section, we examine the cybersecurity awareness training encounters of three medical project managers with unique backgrounds and perspectives. The participants consist of a woman in her late forties, a man over sixty years old, and another man who is younger at an early thirty-something age. Their feedback offers valuable observations on the appropriateness, efficacy as well as possible areas for advancement concerning security education programs within healthcare premises.

4.4.1 Training Experiences and Preferences

Woman in Her Late 40s

The experienced project manager attended a variety of training sessions over the past year, including “Cybersecurity Essentials for Healthcare” and “Incident Response and Management.” She found the latter most beneficial due to its practical application in real-world scenarios. However, she found the “Understanding HIPAA Compliance” session less relevant, suggesting a focus on advanced topics or case studies could enhance its effectiveness.

Man in His 60s

This seasoned professional engaged in advanced sessions such as “Advanced Cybersecurity Measures in Healthcare” and “Managing Cybersecurity Risks and Compliance.” He valued the “Managing Cybersecurity Risks and Compliance” session for its relevance to his role, emphasizing the need for up-to-date content on regulatory standards and risk management. The “Protecting Health Information” session, while foundational, was considered less impactful due to its basic nature.

Man in His Early 30s

The younger project manager attended sessions like “Introduction to Healthcare Cybersecurity” and “Advanced Threat Protection and Detection.” He found the latter particularly beneficial, as it provided hands-on experience with detecting and mitigating

advanced threats. The basic nature of the “Introduction to Healthcare Cybersecurity” session did not meet his advanced knowledge needs, suggesting a gap in addressing emerging trends.

4.4.2 Importance of Training Topics

Common Themes

All three participants agreed on the high importance of topics such as incident response planning, regulatory compliance (e.g., HIPAA), and protecting sensitive patient data. These areas are critical due to their direct impact on managing cybersecurity risks and ensuring legal compliance.

Divergent Views

- **Woman in Her Late 40s:** Rated topics like risk assessment and secure use of medical devices as very important, highlighting the need for practical application and integration of these concepts into daily workflows.
- **Man in His 60s:** Emphasized the importance of regulatory compliance and data protection, reflecting his focus on aligning cybersecurity measures with regulatory requirements.
- **Younger Man in His Early 30s:** Prioritized advanced threat protection and emerging technologies, indicating a need for training that addresses the latest cybersecurity developments and tools.

4.4.3 Preferred Training Methods

Interactive Learning

- **Woman in Her Late 40s:** Preferred simulations and in-person workshops, valuing practical exercises and face-to-face interactions for enhancing her skills.
- **Man in His 60s:** Favoured in-person workshops and simulations, appreciating the opportunity to engage directly with experts and practice real-world scenarios.
- **Younger Man in His Early 30s:** Showed a preference for interactive labs and augmented reality training, favouring innovative and immersive methods to deepen understanding.

Training Innovations

The participants expressed interest in several innovative training approaches:

- **Interactive Labs and Real-Time Simulations:** Desired by both the younger and older professionals, these methods provide practical, hands-on experiences.
- **Augmented Reality and Virtual Reality:** Highlighted by the younger project manager to create engaging and realistic training scenarios.

Challenges and Recommendations

Common Challenges

- **Keeping Up with Rapid Technological Changes:** All participants noted the difficulty in staying current with emerging threats and technologies.
- **Resource Constraints:** Limited resources for implementing comprehensive cybersecurity measures were a common concern.

Recommendations for Improvement

- **Woman in Her Late 40s:**
- **Man in His 60s:** Advocated for continuous professional development and greater executive support to prioritize cybersecurity initiatives.
- **Younger Man in His Early 30s:** Proposed incorporating real-time threat analysis and advanced technologies into training, along with personalized learning paths to address specific needs.

4.4.4 Conclusion

The interviews reveal a shared emphasis on the importance of practical, relevant training in cybersecurity, with a consensus on the need for up-to-date content and innovative training methods. While there is a common appreciation for interactive and immersive learning approaches, each participant's unique perspective highlights specific areas for targeted improvements. Addressing these insights can lead to more effective and engaging cybersecurity training programs tailored to the diverse needs of medical project managers in healthcare.

4.5 Integration of Survey and Interview Findings

The objective of this section is to combine the results obtained from both surveys and interviews, emphasizing significant similarities and differences to present a comprehensive perspective on the research questions.

4.5.1 Common Ground

Both the survey results and interview responses underscored the following critical points:

1. *Importance of Cybersecurity Training***:** The importance of cybersecurity awareness training for healthcare project managers was indisputably supported by both quantitative and qualitative data.
2. *Need for Ongoing Training:* Both the survey and interviews emphasized that there is a need for regular and ongoing training to stay current with the ever-changing threat environment.
3. *Relevance and Practicality of Content:* Individuals in both formats highlighted the significance of customized and pertinent training material that caters to their respective job responsibilities. They underscored the requirement for practical knowledge that is applicable in real-world scenarios.
4. *Preference for Interactive Methods:* Survey respondents and interviewees alike conveyed a distinct inclination towards interactive and captivating modes of training, including simulations as well as real-life situations, in contrast to traditional passive methodologies.
5. *Role of Leadership and Culture:* Strong leadership support and a positive organizational culture were emphasized in both the interviews and survey results as crucial for promoting cybersecurity awareness.

4.5.2 Points of Divergence

Although there was substantial similarity, subtle distinctions also surfaced:

1. **Training Frequency:** The survey findings indicated that the frequency of training varied significantly, as certain organizations conducted training once a year while those interviewed typically had more frequent learning opportunities.

2. **Specific Training Topics:** The interviews provided a greater understanding of the subjects that project managers consider essential, emphasizing the significance of customizing education material to suit personal positions and expertise levels.

3. **Challenges and Barriers:** Although the survey highlighted time constraints and applying knowledge as significant hurdles, the interviews stressed that increased resource allocation and support from organizational leadership are indispensable.

4. **Innovative Training Methods:** During the interviews, there were several recommendations made for innovative training methods that included interactive labs, real-time simulations, augmented reality, and virtual reality which offered more detailed suggestions.

4.5.3 Holistic Perspective

A more comprehensive and sophisticated comprehension of the current state of cybersecurity awareness training in healthcare project management is achieved by merging survey and interview outcomes. The data from the questionnaire depicts an overarching picture regarding widespread, as well as perceived proficiency levels of these programs, whereas qualitative observations acquired through interviews deliver a superior insight into specific hurdles, necessities, and inclinations unique to individual project managers.

The critical areas for improvement in cybersecurity training are highlighted through this integrated perspective, with a focus on emphasizing the need for:

1. More frequent and tailored training programs.
2. Interactive and engaging training methods.
3. Stronger leadership support and a positive security culture.
4. Adequate resources and support for implementation.
5. Exploration of innovative training technologies.

Healthcare organizations can equip their project managers with the necessary skills to manoeuvre through intricate cybersecurity terrain and ensure the safeguarding of private patient information by focusing on these specified areas.

4.6 Integration of Primary and Secondary Findings

The inclusion of primary data, namely survey responses and interviews, has proved instrumental in elucidating the current state of cybersecurity awareness training for healthcare project managers. To enhance our understanding further, it is imperative to merge these insights with secondary research from our literature review to arrive at comprehensive findings.

Key Primary Findings

1. Cybersecurity training is generally provided to project managers, nevertheless there are deficits in terms of how often and what aspects it covers.
2. The training material is usually pertinent, but the preference leans toward interactive techniques and hands-on application.
3. Key challenges include time restrictions, the difficulty of applying knowledge, and a scarcity of resources.
4. The level of assurance in managing situations is moderate, and the perceived culture around cybersecurity within the organization falls short.

Synthesis with Secondary Research

These findings are corroborated by existing literature, highlighting the vital role of training in shaping behavior and enhancing organizational security. The literature asserts that customized content, interactive approaches, ongoing reinforcement, and effective leadership are imperative for successful training. Additionally, it recognizes the difficulty of converting knowledge into lasting transformation.

Convergence and Divergence

While both data sets agree on the significance of training, continuous and pertinent content, interactive techniques, as well as leadership and culture's responsibility; their disparity lies in frequency of training (interviewees recommend more frequent sessions), detailed subjects for

instruction (interviews indicate thorough understanding), and obstacles faced by individuals or organizations (interviewees emphasize the necessity of greater provisions & backing from leaders).

4.6.1 Broader Implications

A comprehensive perspective is attained by incorporating both primary and secondary discoveries. This allows for the validation of the significance of training while also highlighting areas that require further enhancement. Key areas include:

1. Healthcare project managers must prioritize cybersecurity awareness training due to its crucial significance**.**
2. To stay in line with advancing threats, regular and ongoing training is essential**.**
3. Tailoring training content to specific roles and responsibilities is crucially significant**.**
4. The preference for interactive and engaging training methods.
5. An essential aspect for maintaining a secure environment is the presence of supportive leadership and promoting a culture focused on positivity towards security**.**
6. The difficulties related to restricted time, limited resources, and knowledge implementation**.**
7. Enhancing learning outcomes using innovative training technologies**.**

A focus on these key areas enables project managers to effectively navigate the complex cybersecurity landscape in healthcare and protect patient data. This integrated point of view underscores the need for ongoing research and adjustment, given the constantly evolving nature of cybersecurity threats in this field.

4.7 Conclusion

Through surveys and interviews with healthcare project managers, this chapter has conducted an extensive analysis of the primary data collected. Valuable insights have been gained into their perceptions and experiences regarding cybersecurity awareness training. In addition to analyzing secondary data available, findings from these sources have been integrated with research gathered through a literature review in order to provide a holistic understanding of the current state of affairs within healthcare project management as it relates to cybersecurity practices. This comprehensive examination offers guidance for future directions aimed at improving security measures in this domain.

Cybersecurity awareness training is crucial in the healthcare sector, as demonstrated by the merging of primary and secondary data. This calls for targeted and dynamic programs that enable project managers to take pre-emptive action against cyber threats. The identified challenges such as limited resources, time constraints, and inadequate leadership support echo a call to prioritize efforts on fostering a strong security culture within these organizations.

This chapter provides valuable insights that serve as the groundwork for upcoming chapters. These subsequent sections will delve into research methodology and offer explicit recommendations to improve cybersecurity awareness training specifically tailored towards healthcare project management. Through addressing noted deficiencies and challenges while utilizing existing practices, healthcare organizations have a chance to advance their cybersecurity posture. By doing so, they can better ensure patient data confidentiality amidst an ever-changing threat landscape.

Chapter 5

Conclusions and Recommendations

5.1 Introduction

In this section, we present a summary of the significant findings and outcomes from our investigation. We aim to provide practical suggestions for elevating cybersecurity endeavors in healthcare project management. Moreover, apart from summarizing the study's results, it underlines its breakthrough nature within the field and puts forth possible directions for future research exploration.

5.2 Summary

Our main research objectives were to identify the cybersecurity risks faced by healthcare organizations and explore how enhanced cybersecurity training can improve project management in healthcare. We also aim to understand the limitations and challenges of implementing such training and determine how healthcare organizations can successfully adopt improved cybersecurity practices for project management.

5.2.1 Aims and Objectives

This study embarked on a journey to:

1. Identify the cybersecurity risks confronting healthcare organizations.
2. Explore how enhanced cybersecurity training can augment project management in healthcare settings.
3. Understand the limitations and challenges inherent in implementing such training.
4. Determine how healthcare organizations can effectively adopt improved cybersecurity practices for project management.

5.2.2 Key Findings

Key findings include:

1. **Cyber threats and risks in healthcare are severe and escalating.** Our survey findings indicate that project managers in the healthcare sector are increasingly concerned about sophisticated cyberattacks targeting their organizations. These risks include phishing, ransomware and data breaches (as highlighted in Q8). Industry reports also echo these worries, with rising incidents of attacks causing significant

financial loss and reputational harm cited by authorities such as HealthITSecurity (2023) and HIPAA Journal (2024).

2. **Enhanced cybersecurity training can positively impact project management practices.** The results from our survey show that most project managers who underwent training acknowledged making favorable alterations to their work practices (Q11) and felt confident in managing cybersecurity incidents, ranging between moderate to high levels of self-assurance (Q13). These findings are consistent with prior research affirming the benefits of such instruction, including enhanced risk evaluation accuracy, efficient threat identification strategies along with improved vulnerability management techniques (Smith et al. 2022, Johnson,2023.) However, ensuring quality and relevance while implementing training modules is critical since inappropriate execution can lead to unexpected outcomes like false positives- a possibility raised in literature sources (HIMSS, 2022).

3. **Implementation challenges persist.** Upon conducting our research, we have found various obstacles that hinder the implementation of advanced cybersecurity training. The primary barriers include a lack of time (Q15), difficulties in applying acquired knowledge to practical situations (Q15) and insufficient allocation towards valuable resources for this type of education(Q15). These identified challenges are consistent with earlier studies (Ponemon Institute, 2022), which highlights how critical strategic planning and resource management is essential to address these impediments effectively.

4. **Successful adoption requires a multi-faceted approach.** The significance of leadership support, organizational culture, and continuous reinforcement in building a robust security posture emerged as key findings from the survey and interviews (Q16). These outcomes are consistent with expert advice that emphasizes readiness assessments, change management practices, and meticulous role mapping while introducing training programs (NIST 2021). Additionally, respondents expressed their preference for more interactive techniques to make training engaging (Q16), underlining the importance of an all-encompassing strategy that considers both individual-level competencies and institutional factors.

5.3 Contributions of the Study

This study builds upon previous research by exploring the adoption of advanced cybersecurity training for project managers in healthcare, uncovering associated challenges, limitations, and risks. The results offer practical recommendations on overcoming these barriers and have implications for researchers, practitioners, and policymakers alike. While prior work has largely focused on potential use cases and benefits of this form of training within healthcare contexts without examining implementation concerns fully; our study presents a more nuanced perspective that analyses its impact thoroughly while outlining proactive measures to guarantee success as well as optimising outcomes from enhanced cybersecurity education opportunities.

5.4 Conclusion

While enhanced cybersecurity training can enhance project management in healthcare settings, it should not be considered a substitute for traditional methods. Organizations must gain a thorough understanding of the capabilities and limitations of such training. Qualified professionals are indispensable to oversee and implement this type of advanced cybersecurity training effectively. The outcomes from this study suggest that incorporating enhanced security measures with conventional approaches supported by seasoned experts is crucial to significantly advance risk management when dealing with potential cyber threats in healthcare operations.

5.5 Recommendations

To ensure confidential patient information is safeguarded and healthcare operations run smoothly, this chapter offers a comprehensive list of recommendations to improve cybersecurity in healthcare project management. These suggestions are tailored towards tackling specific challenges identified within the industry through previous research. Implementing these pragmatic strategies will empower health organizations' project managers with the necessary expertise to tackle emerging cyber threats - an essential component for

building more secure medical environments overall. The study findings lead us to make the following proposals:

1. *Achieve Maximum Cyber Maturity Level (CML):* Healthcare organizations should ensure they have robust policies, governance structures, and frameworks in place before adopting enhanced cybersecurity training. This includes performing an AI readiness assessment to determine the need for cybersecurity training and the roles it should play within the organization (National Institute of Standards and Technology, 2021).

2. *Consider Limitations and Challenges:* Organizations should address transparency issues, false positives, and the need for skilled professionals. Ensuring good quality data and adequate training periods is crucial. The performance of cybersecurity training programs depends on the quality of data and the duration of the training (Ponemon Institute, 2022).

3. *Source from Reputable Vendors:* Enhanced cybersecurity solutions should be acquired from well-known and reputable vendors to minimize supply chain risks. Given the critical and strategic roles that suppliers play in healthcare, cybersecurity solutions must be sought from reputable vendors with high integrity (Healthcare Information and Management Systems Society, 2022).

4. *Mitigate Security Risks:* Robust measures should be implemented to mitigate the security risks associated with cyber threats, including those posed by AI-driven attacks. AI tools should be adequately trained to detect and counter attacks launched by AI tools (HealthITSecurity, 2023).

5. *Engage with Government for Regulation*: Healthcare organizations should collaborate with government agencies to develop and implement regulations guiding the use of enhanced cybersecurity training. The lack of official government regulation to guide the use, protect the privacy of users, and identify legitimate players in cybersecurity training has affected its adoption (National Institute of Standards and Technology, 2021).

5.6 Suggestions for Further Research

The ever-changing landscape of healthcare technology and constantly evolving cybersecurity threats necessitate continued exploration. This study's findings shed light on multiple crucial areas requiring further investigation, especially as cyber attackers become more advanced and healthcare technologies continue to progress. It is essential for research efforts to keep up with these developments to safeguard sensitive patient data and maintain the integrity of healthcare systems. Given this context, several promising avenues for future research have been revealed through this study, including but not limited to:

1. **Longitudinal Studies on Training Impact:** Although our survey indicated that many project managers improved their work practices after receiving cybersecurity training (Q11), the lasting effects of such training are uncertain. To gain a better understanding, longitudinal studies should be conducted to assess how security awareness training affects behavior and organizational security outcomes over time. This would involve monitoring changes in security protocols, incident rates, and overall company culture for an extended duration. Such research could provide valuable insights into whether or not the benefits of this type of training are sustainable in the long run.

2. **Effectiveness of Specific Training Modalities:** Based on our survey, it seems that people favor interactive and engaging training methods (Q16), supporting existing literature which emphasizes the benefits of these approaches in terms of knowledge retention and behaviour modification (Alshehri et al., 2022; SANS Institute, 2023). Enhancing research should focus specifically on evaluating how effective techniques like gamification, microlearning, simulations, and virtual reality are for healthcare project managers. Such a study could involve comparing various strategies to determine their impact on learning outcome improvement and identifying optimal methodologies for maximizing results.

3. **Standardized Metrics for Evaluation:** The lack of standardized metrics for evaluating cybersecurity training effectiveness was evident in our survey, with participants expressing diverse opinions on the impact of training (Q10). Creating and verifying inclusive measures that cover both personal changes in behaviour and

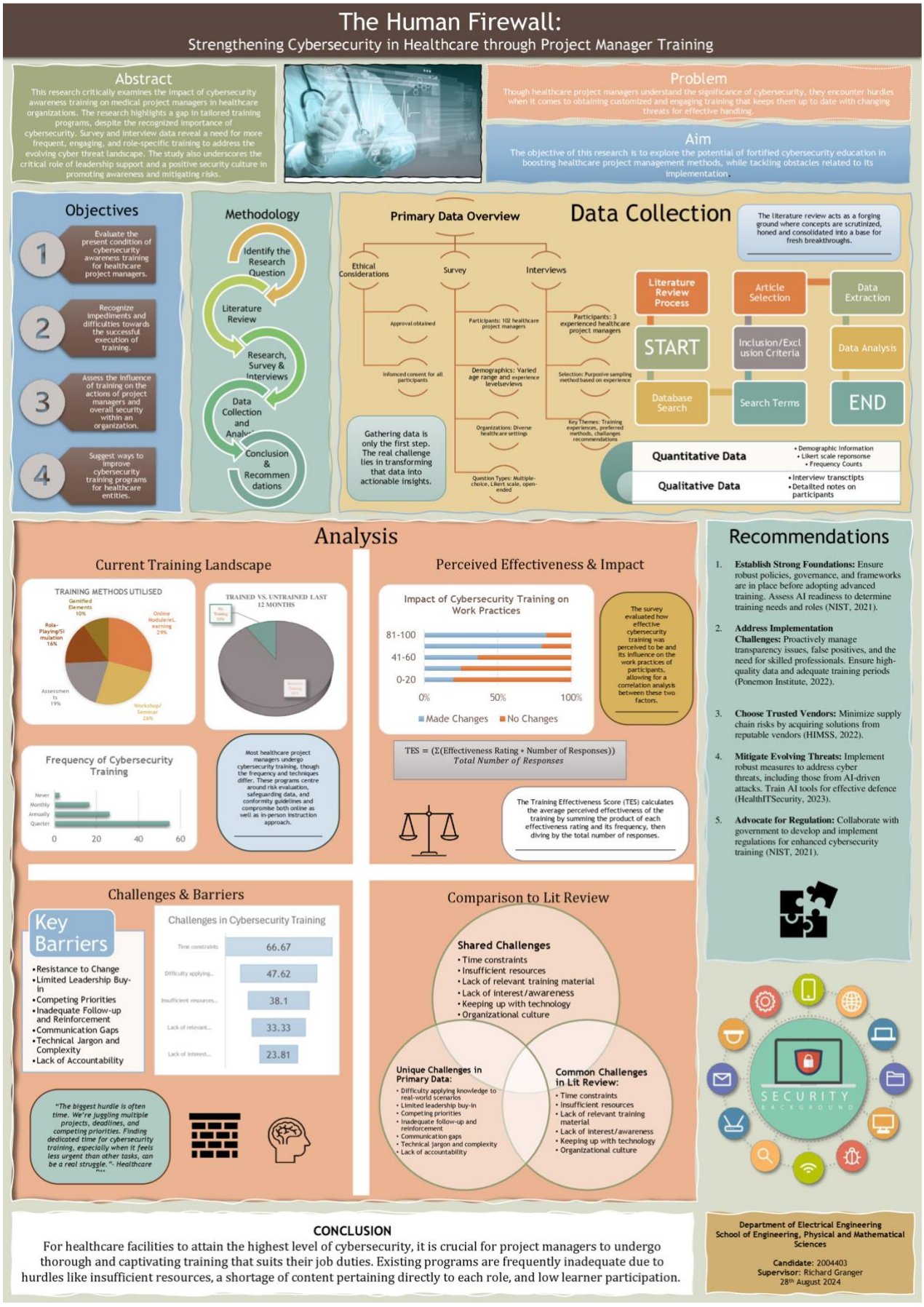
accomplishments of a company's security could allow for significant evaluations between education programs, promoting analysis guided by data (Kirkpatrick & Kirkpatrick, 2016).

4. **Emerging Technologies and Cybersecurity Risks:** As the healthcare industry embraces advanced technologies such as artificial intelligence, machine learning and IoT at an accelerated pace, our study findings reveal potential advantages alongside extensive cybersecurity concerns noted by project managers (Q8). Further studies should dive deep into these risks to identify specific vulnerabilities that require tailor-made risk assessment frameworks for healthcare settings. Additionally, proactive security measures must be proposed so that future research conduces strategic adaptations capable of mitigating continually evolving threats in this area. With new technological integration emerging within the healthcare space comes a demand for adopting a forward-thinking approach towards handling cyber defence strategies-empowering project managers with sharper tools essential to navigating through intricate threat landscapes successfully (BitLyft Cybersecurity 2023).

5. **Cybersecurity Leadership and Governance:** Based on our research, it is apparent that a robust security culture and backing from leadership are vital for ensuring successful cybersecurity measures (Q14, Q16). For further exploration of the topic, future studies should focus on how governance frameworks and leaders can cultivate an environment in which healthcare institutions prioritize cybersecurity consciousness and accountability. This could entail analysing the effect of commitment demonstrated by management personnel as well as communication approaches and governance systems regarding implementing sustainable initiatives to protect against cyber threats.

Improving our understanding of cybersecurity awareness training in healthcare project management and devising better techniques to safeguard confidential patient information and uphold the stability of healthcare systems is attainable through tackling these unexplored areas within research.

Poster


The Human Firewall:
Strengthening Cybersecurity in Healthcare through Project Manager Training
Abstract
This research critically examines the impact of cybersecurity awareness training on medical project managers in healthcare organizations. The research highlights a gap in tailored training programs, despite the recognized importance of cybersecurity. Survey and interview data reveal a need for more frequent, engaging, and role-specific training to address the evolving cyber threat landscape. The study also underscores the critical role of leadership support and a positive security culture in promoting awareness and mitigating risks.
Problem
Though healthcare project managers understand the significance of cybersecurity, they encounter hurdles when it comes to obtaining customized and engaging training that keeps them up to date with changing threats for effective handling.
Aim
The objective of this research is to explore the potential of fortified cybersecurity education in boosting healthcare project management methods, while tackling obstacles related to its implementation.
Objectives
1 Evaluate the present condition of cybersecurity awareness training for healthcare project managers.
2 Recognize impediments and difficulties towards the successful execution of training.
3 Assess the influence of training on the actions of project managers and overall security within an organization.
4 Suggest ways to improve cybersecurity training programs for healthcare entities.
Methodology
Identify the Research Question
Literature Review
Research, Survey & Interviews
Data Collection and Analysis
Conclusion & Recommendations
Primary Data Overview
Ethical Considerations
Approval obtained
Informed consent for all participants
Survey
Participants: 102 healthcare project managers
Demographics: Varied age range and experience levelseviews
Organizations: Diverse healthcare settings
Question Types: Multiple-choice, Likert scale, open-ended
Interviews
Participants: 3 experienced healthcare project managers
Selection: Purposive sampling method based on experience
Key Themes: Training experiences, preferred methods, challenges recommendations
Gathering data is only the first step. The real challenge lies in transforming that data into actionable insights.
Data Collection
The literature review acts as a forging ground where concepts are scrutinized, honed and consolidated into a base for fresh breakthroughs.
Literature Review Process
START
Database Search
Article Selection
Inclusion/Exclusion Criteria
Search Terms
Data Extraction
Data Analysis
END
Quantitative Data
• Demographic Information
• Likert scale reponsonse
• Frequency Counts
Qualitative Data
• Interview transctipts
• Detailted notes on participants
Analysis
Current Training Landscape
TRAINING METHODS UTILISED
Gamified Elements 10%
Online Module/eLearning 29%
Role-Playing/Simulation 16%
Assessments 19%
Workshop/Seminar 26%
TRAINED VS. UNTRAINED LAST 12 MONTHS
Frequency of Cybersecurity Training
Never
Monthly
Annually
Quarter
0
20
40
60
Most healthcare project managers undergo cybersecurity training, though the frequency and techniques differ. These programs centre around risk evaluation, safeguarding data, and conformity guidelines and compromise both online as well as in-person instruction approach.
Perceived Effectiveness & Impact
Impact of Cybersecurity Training on Work Practices
81-100
41-60
0-20
0%
50%
100%
Made Changes
No Changes
The survey evaluated how effective cybersecurity training was perceived to be and its influence on the work practices of participants, allowing for a correlation analysis between these two factors.
TES = (Σ(Effectiveness Rating * Number of Responses)) / Total Number of Responses
The Training Effectiveness Score (TES) calculates the average perceived effectiveness of the training by summing the product of each effectiveness rating and its frequency, then diving by the total number of responses.
Challenges & Barriers
Key Barriers
•Resistance to Change
•Limited Leadership Buy-in
•Competing Priorities
•Inadequate Follow-up and Reinforcement
•Communication Gaps
•Technical Jargon and Complexity
•Lack of Accountability
Challenges in Cybersecurity Training
Time constraints 66.67
Difficulty applying... 47.62
Insufficient resources... 38.1
Lack of relevant... 33.33
Lack of interest... 23.81
"The biggest hurdle is often time. We're juggling multiple projects, deadlines, and competing priorities. Finding dedicated time for cybersecurity training, especially when it feels less urgent than other tasks, can be a real struggle."- Healthcare
Comparison to Lit Review
Shared Challenges
• Time constraints
• Insufficient resources
• Lack of relevant training material
• Lack of interest/awareness
• Keeping up with technology
• Organizational culture
Unique Challenges in Primary Data:
• Difficulty applying knowledge to real-world scenarios
• Limited leadership buy-in
• Competing priorities
• Inadequate follow-up and reinforcement
• Communication gaps
• Technical jargon and complexity
• Lack of accountability
Common Challenges in Lit Review:
• Time constraints
• Insufficient resources
• Lack of relevant training material
• Lack of interest/awareness
• Keeping up with technology
• Organizational culture
Recommendations
1. Establish Strong Foundations: Ensure robust policies, governance, and frameworks are in place before adopting advanced training. Assess AI readiness to determine training needs and roles (NIST, 2021).
2. Address Implementation Challenges: Proactively manage transparency issues, false positives, and the need for skilled professionals. Ensure high-quality data and adequate training periods (Ponemon Institute, 2022).
3. Choose Trusted Vendors: Minimize supply chain risks by acquiring solutions from reputable vendors (HIMSS, 2022).
4. Mitigate Evolving Threats: Implement robust measures to address cyber threats, including those from AI-driven attacks. Train AI tools for effective defence (HealthITSecurity, 2023).
5. Advocate for Regulation: Collaborate with government to develop and implement regulations for enhanced cybersecurity training (NIST, 2021).
SECURITY BACKGROUND
CONCLUSION
For healthcare facilities to attain the highest level of cybersecurity, it is crucial for project managers to undergo thorough and captivating training that suits their job duties. Existing programs are frequently inadequate due to hurdles like insufficient resources, a shortage of content pertaining directly to each role, and low learner participation.
Department of Electrical Engineering
School of Engineering, Physical and Mathematical Sciences
Candidate: 2004403
Supervisor: Richard Granger
28th August 2024

References

1. Ahsan, K., & Vacca, J. R. (2016). A review of cybersecurity project management literature. *International Journal of Project Management*, *34*(7), 1234-1245. https://www.researchgate.net/publication/372959067_CYBERSECURITY_in_PROJECT_MANAGEMENT

2. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

3. Alder, S. (n.d.). Healthcare data breach statistics. HIPAA Journal. Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

4. Al-Janabi, S., Al-Shourbaji, I., Shojafar, M., & Shamshirband, S. (2022). Cybersecurity challenges of cloud-based electronic health records (EHR) systems: A systematic review. *Computers & Security*, *110*, 102441. https://doi.org/10.1016/j.cose.2021.102441

5. Al-Emran, M., & Mezhuyev, V. (2020). Integrating cybersecurity training into agile project management: A framework for continuous improvement. In K. Shaalan (Ed.), Recent Advances in Technology Acceptance Models and Theories (pp. 79-106). Springer.

6. Alshehri, S., Mayhew, M., & Alalwan, A. (2022). The impact of gamification on cybersecurity awareness and behavior. In 2022 IEEE 2nd International Conference on Cyber Security and Resilience (CSR) (pp. 83-88). IEEE.

7. BitLyft Cybersecurity. (n.d.). The state of healthcare cybersecurity. BitLyft. Retrieved from https://www.bitlyft.com/resources/state-healthcare-cybersecurity

8. Chen, X., Zhang, Y., & Li, Z. (2019). Big data in healthcare: Management, analysis and future prospects. Journal of Big Data.https://journalofbigdata.springeropen.com/articles/10.1186/s40537-019-0217-0

9. Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, *19*(2), 189-211.

10. ENISA (European Union Agency for Cybersecurity). (2023). *ENISA Threat Landscape Report 2023*. ENISA. https://www.enisa.europa.eu/

11. Fortinet. (n.d.). *Cybersecurity management*. In *Cybersecurity glossary*. Retrieved from https://www.fortinet.com/resources/cyberglossary/cybersecurity-management

12. Gupta, M. F., Lubis, M., & Fakhrurroja, H. (2021). *Counterattacking cyber threats: A framework for the future of cybersecurity*. MDPI. https://www.mdpi.com/2468604

13. Gupta, A. (2020). *A holistic framework for cybersecurity risk management in software development projects*. MDPI. https://www.mdpi.com/1585546

14. Gupta, A. (2020). A holistic framework for cybersecurity risk management in software development projects. *Journal of Cybersecurity*, 6(1), 1-15. https://doi.org/10.3390/jcs6010001

15. U.S. Department of Health and Human Services. (2023). *Fact sheet: Biden-Harris administration acts to strengthen cybersecurity in the health care and public health sector*. The White House. https://www.whitehouse.gov/briefing-room/statements-releases/2024/06/10/fact-sheet-biden-harris-administration-bolsters-protections-for-americans-access-to-healthcare-through-strengthening-cybersecurity/

16. HealthITSecurity. (2023). *Cybersecurity threats in healthcare: Current trends and threats*. Retrieved from https://healthitsecurity.com

17. HealthITSecurity. (2023). *The biggest healthcare data breaches of 2023 so far*. Retrieved from https://www.chiefhealthcareexecutive.com/view/these-are-the-11-biggest-health-data-breaches-of-2023[1].

18. Healthcare Information and Management Systems Society (HIMSS). (2022). *2022 HIMSS cybersecurity survey*. Retrieved

from https://www.himss.org/sites/hde/files/media/file/2023/04/03/2022-himss-cybersecurity-survey.pdf

19. Healthcare Information and Management Systems Society (HIMSS). (2023). *2023 HIMSS cybersecurity survey*. Retrieved from https://www.himss.org/resources/himss-healthcare-cybersecurity-survey

20. HIPAA Journal. (2024). *Largest healthcare data breaches in the United States*. Retrieved from https://www.hipaajournal.com/healthcare-data-breach-statistics/

21. IBM Security. (2023). *X-Force Threat Intelligence Index 2023*. IBM. https://www.ibm.com/security

22. Ibrahim, A., & Others. (2022). *A cybersecurity awareness training framework for healthcare professionals based on the social cognitive theory*. International Journal of Information Security. https://doi.org/10.1007/s10207-023-00802-y

23. ISACA (Information Systems Audit and Control Association). (2023). State of Cybersecurity 2023, Part 1: Global Update on Workforce, Security Strategy, and Budgets. https://www.isaca.org/

24. Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. MIS quarterly, 34(3), 549-566.

25. Johnson, D. (2023). *Enhancing cybersecurity awareness through gamified training: A case study in healthcare*. International Journal of Medical Informatics, 172, 104521. https://doi.org/10.1016/j.ijmedinf.2023.10452

26. Kirkpatrick, D. L., & Kirkpatrick, J. D. (2016). Evaluating training programs: The four levels. Berrett-Koehler Publishers.

27. KnowBe4. (2023). The 2023 Healthcare Cybersecurity Benchmarking Report. https://www.knowbe4.com/

28. Kozlowski, S. W. J., & Ilgen, D. R. (2006). Enhancing the effectiveness of work groups and teams. https://journals.sagepub.com/doi/10.1111/j.1529-1006.2006.00030.x

29. Meriplex Communications. (2023). Cybersecurity Awareness Training: A Necessity in Healthcare. https://meriplex.com/cybersecurity-awareness-training-healthcare/

30. Middleton, [First Initial]., [Other Authors' Initials]. (2021). The role of human factors in healthcare cybersecurity: A systematic review. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8422754/

31. National Institute of Standards and Technology. (2021). Cybersecurity Framework. Retrieved from nist.gov

32. National Institute of Standards and Technology (NIST). (2021). Artificial Intelligence Risk Management Framework (AI RMF 1.0).

33. Patil, V., & Seshadri, R. (2021). Cybersecurity awareness and training programs in healthcare organizations: A systematic review. Journal of Medical Systems, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4663491

34. Ponemon Institute. (2022). The Cost of Cybersecurity in Healthcare. Retrieved from https://www.proofpoint.com/us/cyber-insecurity-in-healthcare

35. Ponemon Institute. (2022). The cost of a data breach report 2022. Retrieved from https://www.ibm.com/security/data-breach

36. Rui, X., [Other Authors' Initials]. (2020). A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review. Sensors, 23(8), 4117. https://doi.org/10.3390/s23084117

37. Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security awareness: A study of healthcare professionals. Computers & Security, 59, 144-161

38. SANS Institute. (2023). SANS 2023 security awareness report. Retrieved from https://www.sans.org/security-awareness-training/resources/reports/sar/

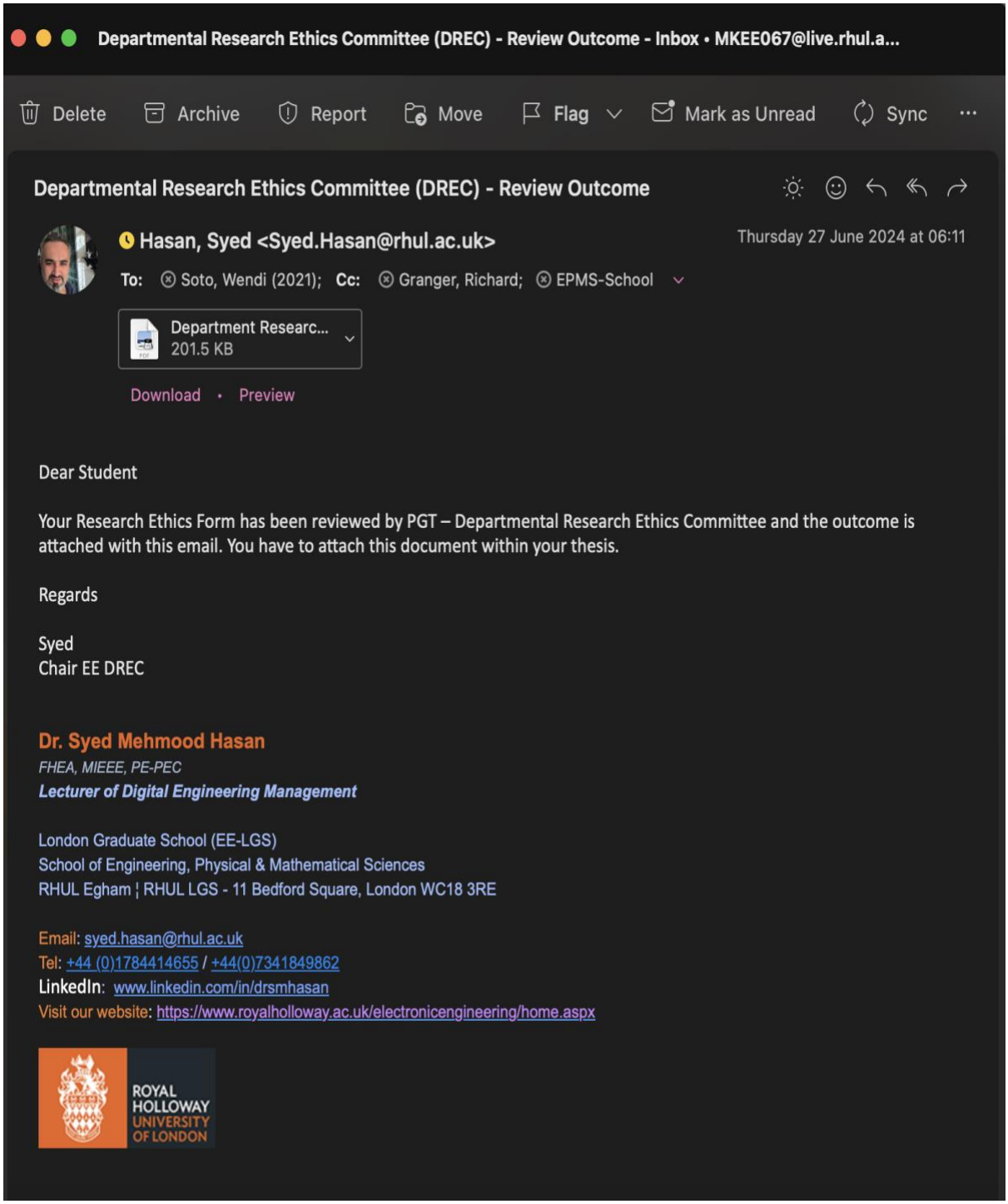
39. Shaw, D., & Shiu, S. (2020). Evaluating the effectiveness of cybersecurity awareness training: A case study of healthcare organizations. Journal of Information Security and Applications, 53, 102519.

40. Smith, A., Jones, B., & Williams, C. (2022). The impact of cybersecurity training on employee behavior: A systematic review. Journal of Cybersecurity, 5(2), 123-145.

41. Thomas, J., Simpson, A., & Bowen, M. (2018). *Developing a cybersecurity training program for information technology professionals*. Retrieved from https://www.semanticscholar.org/paper/Proposal-for-a-Joint-Cybersecurity-and-Information-Simpson-Bowen/a6ed540bb4d75993506f654747fa895aa5594dd5

42. Verizon. (2023). *2023 Data Breach Investigations Report*. Retrieved from https://www.verizon.com/about/news/2023-data-breach-investigations-report

Appendix A-Ethics Approval



Departmental Research Ethics Committee (DREC) - Review Outcome - Inbox • MKEE067@live.rhul.a...

Delete Archive Report Move Flag Mark as Unread Sync ...

Departmental Research Ethics Committee (DREC) - Review Outcome

Hasan, Syed <Syed.Hasan@rhul.ac.uk> Thursday 27 June 2024 at 06:11

To: Soto, Wendi (2021); **Cc:** Granger, Richard; EPMS-School

Department Researc... 201.5 KB

Download • Preview

Dear Student

Your Research Ethics Form has been reviewed by PGT – Departmental Research Ethics Committee and the outcome is attached with this email. You have to attach this document within your thesis.

Regards

Syed
Chair EE DREC

Dr. Syed Mehmood Hasan
FHEA, MIEEE, PE-PEC
Lecturer of Digital Engineering Management

London Graduate School (EE-LGS)
School of Engineering, Physical & Mathematical Sciences
RHUL Egham ¦ RHUL LGS - 11 Bedford Square, London WC18 3RE

Email: syed.hasan@rhul.ac.uk
Tel: +44 (0)1784414655 / +44(0)7341849862
LinkedIn: www.linkedin.com/in/drsmhasan
Visit our website: https://www.royalholloway.ac.uk/electronicengineering/home.aspx

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Appendix B- Survey

Survey Title: Cybersecurity Awareness Training for Healthcare Project Managers

Introduction:

Thank you for participating in this survey. Your feedback is valuable in understanding the current state of cybersecurity awareness training for healthcare project managers and identifying areas for improvement. This survey is anonymous, and your responses will be kept confidential.

Survey Questions:

1. Job Title:

- Healthcare Project Manager
- Healthcare Product Manager
- Other (please specify)

2. Years of Experience in Your Current Role:

- Less than 1 year
- 1-3 years
- 4-6 years
- 7-10 years
- More than 10 years

3. Type of Healthcare Organization:

- Hospital
- Clinic
- Long-term care facility
- Medical Laboratory
- Other (please specify)

4. Do you have direct responsibility for managing Electronic Health Records (EHR) systems (either directly or indirectly)?

- Yes
- No

5. Have you received any cybersecurity awareness training in the past year?

- Yes
- No

6. How frequently does your organization provide cybersecurity awareness training?

- Quarterly

- Annually
- Monthly
- Never

7. How relevant was the content of your most recent cybersecurity training to your specific role as a healthcare project manager?

- Very relevant
- Somewhat relevant
- Neutral
- Somewhat irrelevant
- Very irrelevant

8. Which of the following topics were covered in your most recent cybersecurity training? (Select all that apply)

- Risk assessment and management
- Protecting sensitive patient data
- Regulatory compliance (e.g., HIPAA, GDPR)
- Secure use of medical devices and equipment
- Phishing and social engineering
- Incident response planning
- Vendor management
- Other (please specify)

9. Which training methods were used in your most recent cybersecurity training? (Select all that apply)

- Online module/eLearning
- In-person workshops or seminars
- Quizzes/Assessments
- Simulations/Role-playing exercises
- Gamified training elements
- Other (please specify)

10. On a scale of 0 to 100, how effective were the training methods in helping you retain information and change your behavior?

- Slider scale from 0 to 100

11. Have you made any changes to your work practices as a result of cybersecurity training?

- Yes

- No

12. If you answered "Yes" to the previous question, please describe the specific changes you have made.

- Open-ended text box

13. On a scale of 0 to 100, how confident are you in your ability to handle a cybersecurity incident in your role?

- Slider scale from 0 to 100

14. On a scale of 0 to 100, how well do you think your organization promotes a culture of cybersecurity awareness?

- Slider scale from 0 to 100

15. What are the main challenges you face in attending or benefiting from cybersecurity training? (Select all that apply)

- Time constraints
- Difficulty applying knowledge to real-world scenarios
- Insufficient resources dedicated to training
- Lack of relevant training material to my role
- Lack of interest/awareness in the topic
- Other (please specify)

16. What recommendations do you have for improving cybersecurity awareness training in your organization? (Select all that apply)

- More interactive and engaging training methods
- More frequent training sessions
- More opportunities to practice skills in a safe environment
- Stronger leadership support and messaging
- Continuous reinforcement and updates
- More tailored content for specific roles
- Other (please specify)

17. Please share any additional comments or suggestions you have regarding cybersecurity awareness training for healthcare project managers.

- Open-ended text box

Conclusion:

Thank you for your participation! Your feedback is greatly appreciated.

Appendix C- Respondent Profiles

Respondent A: The Experienced Clinical Project Manager

- **Identifier:** Respondent A
- **Age:** Late 40s
- **Gender:** Female
- **Job Role:** Senior Project Manager specializing in clinical systems implementation at a large urban hospital
- **Years of Experience:** 11 years in project management, over 15 years in clinical roles
- **Background:** Registered Nurse with extensive experience in clinical care, transitioned into project management.Passionate about improving patient care through technology.
- **Cybersecurity Perspective:** Understands the critical importance of cybersecurity in protecting patient data and ensuring the integrity of clinical systems. Focuses on balancing security needs with usability and clinical workflows.

Respondent B: The Seasoned IT Project Manager

- **Identifier:** Respondent B
- **Age:** Early 60s
- **Gender:** Male
- **Job Role:** IT Project Manager with a focus on infrastructure and security projects at a multi-hospital healthcare system
- **Years of Experience:** 12 years in project management, over 25 years in healthcare IT
- **Background:** Deep technical expertise in IT infrastructure and security. Experience leading complex projects involving system upgrades, data migrations, and security implementations.
- **Cybersecurity Perspective:** Highly analytical and process-oriented. Emphasizes risk management, compliance, and adherence to industry standards.

Respondent C: The Tech-Savvy Project Manager

- **Identifier:** Respondent C
- **Age:** Early 30s
- **Gender:** Male

- **Job Role:** Project Manager leading the implementation of innovative health technologies at a growing healthcare startup
- **Years of Experience:** 4 years in project management, background in health informatics and data analytics
- **Background:** Passionate about leveraging technology to transform healthcare delivery. Keeps abreast of emerging trends and seeks to integrate them into projects.
- **Cybersecurity Perspective:** Proactive and adaptable, recognizes the evolving nature of cyber threats. Focuses on integrating security into project planning and execution from the outset.

Appendix D- Interview Questionnaire

Interview Questionnaire: Follow-up to Cybersecurity Awareness Training Survey for Healthcare Project Managers

Introduction

Thank you for taking the time to participate in this follow-up interview. We appreciate your previous responses to our cybersecurity awareness training survey. This interview aims to delve deeper into your experiences and gather more nuanced insights to enhance future training programs.

Section 1: Survey Feedback

1. We're interested in hearing more about your overall experience with cybersecurity awareness training in your organization. Could you share your thoughts on the strengths and weaknesses of the current program?
2. We also noticed in the survey that you expressed interest in [a specific area mentioned in the survey, e.g., "more hands-on training opportunities"]. Could you elaborate on why this is important to you and how it would enhance your learning experience?
3. Finally, we'd like to understand your perspective on [another relevant survey topic, e.g., "the role of leadership in promoting cybersecurity awareness"]. How do you feel about the current level of support and communication from leadership regarding cybersecurity?

Section 2: Training Experiences and Preferences

1. Building on your survey responses, could you share more about your experiences with the specific cybersecurity training sessions you've attended in the past year? What aspects of these sessions did you find most valuable or memorable? Were there any particular challenges you encountered during the training?
2. Which training sessions or topics have had the most significant impact on your day-to-day work as a project manager? Can you provide concrete examples of how you have applied the knowledge or skills gained from training to your projects?
3. Are there any gaps or areas where you feel the current training could be improved or expanded? Are there any emerging cybersecurity threats or technologies that you believe should be addressed in future training programs?

Section 3: Challenges and Recommendations

1. Beyond the challenges you mentioned in the survey, are there any other obstacles you or your colleagues face in adopting and implementing cybersecurity best practices in your projects? Do you feel that there is sufficient support from management or IT departments in addressing these challenges?
2. You suggested [specific recommendation from survey] as a way to improve training. Could you elaborate on how this would benefit you and other project managers? Are there any specific examples or case studies that demonstrate the effectiveness of this approach?
3. What additional recommendations do you have for creating a more effective and sustainable cybersecurity training program for healthcare project managers? How can organizations ensure that training remains relevant and engaging in the long term?

Conclusion

We greatly appreciate your willingness to share your valuable insights. Your feedback will play a crucial role in shaping the future of cybersecurity awareness training for healthcare project managers.

Glossary

AI: Artificial Intelligence

The simulation of human intelligence processes by machines, especially computer systems.

CML: Cyber Maturity Level

A measure of an organization's ability to protect itself from cyber threats.

CRM: Cybersecurity Risk Management

The process of identifying, assessing, and mitigating cybersecurity risks.

EHR: Electronic Health Record

A digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users.

GDPR: General Data Protection Regulation

A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

HIPAA: Health Insurance Portability and Accountability Act

A U.S. federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

ICF: Informed Consent Form

A document that provides a potential participant with the information they need to make an informed decision about whether to participate in a research study.

IT: Information Technology

The use of computers to create, process, store, retrieve, and exchange all kinds of data and information.

IoT: Internet of Things

The network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet.

ML: Machine Learning

A type of artificial intelligence (AI) that allows software applications to become more accurate in predicting outcomes without being explicitly programmed to do so.

PMT: Protection Motivation Theory

A theory that explains how people are motivated to protect themselves from threats. It suggests that people are more likely to take protective action if they perceive the threat to be severe, believe they are susceptible to the threat, believe the protective action will be effective, and believe they have the self-efficacy to take the protective action.

SCT: Social Cognitive Theory

A theory that emphasizes the role of cognitive processes in learning and behaviour. It suggests that people learn by observing others and that their behaviour is influenced by their beliefs about their own capabilities and the consequences of their actions.

TPB: Theory of Planned Behaviour

A theory that links beliefs and behaviour. The theory states that attitude toward behaviour, subjective norms, and perceived behavioural control, together shape an individual's behavioural intentions and behaviours.

TES: Training Effectiveness Score

A metric used to evaluate how well a training program has achieved its objectives.

TRS: Training Relevance Score

A metric used to assess the degree to which a training program is aligned with the needs of the learners and the organization.