

Midocean University

Faculty of Management

Bachelor of Project Management



The Effect of Cybersecurity Awareness Training on Employee Knowledge and Behavior

Abubaker Hussain Alattas

2021202957

Final Project - 2

Faculty of Management - Midocean University

Supervisor

Dr. Mona Moustafa Elashry

Faculty Member - Faculty of Management - Midocean University

June 29, 2024 – 2nd Trimester 2024

Acknowledgment

I would like to extend my sincere gratitude to the following individuals and organizations for their invaluable contributions to this research:

- **My Supervisor and Academic Advisor:**

Dr. Mona Moustafa Elashry, for her unwavering support, guidance, and constructive feedback throughout the research process. Her expertise and insights were instrumental in shaping this study.

- **The Head of Cybersecurity & Data Management:**

Talal Samy Al Ali, for his invaluable assistance and insights into the cybersecurity aspects of the study. His expertise and support greatly enhanced the depth and relevance of the research.

- **The Research Participants:**

The employees of Allianz Saudi Fransi Insurance Company who took the time to participate in the survey and interviews. Your willingness to share your experiences and insights was crucial to the success of this research.

- **Institutional Support:**

Allianz Saudi Fransi Insurance Company, for providing the necessary resources and support to conduct this research. The company's commitment to cybersecurity and employee training has been a key factor in the study's relevance and impact.

- **Classmates, Student Forum Team:**

My classmates and members of the Student Forum team, for their support, feedback, and camaraderie throughout this research journey. Your collective insights and encouragement were invaluable.

- **Family and Friends:**

For their patience, understanding, and encouragement during the research process. Your support has been a constant source of motivation.

Thank you all for your contributions and support. This research would not have been possible without your help.

Dedication

This research is dedicated to the following individuals who have been instrumental in my journey:

To my family, whose unwavering love, encouragement, and sacrifices have been my foundation. Your belief in my abilities has fueled my determination and resilience throughout this research.

To my friends, whose support, understanding, and camaraderie have provided both comfort and motivation. Your encouragement has been a source of strength, helping me to persevere through the challenges.

To my mentors, including Dr. Mona Moustafa Elashry and Talal Samy Al Ali, whose guidance and expertise have been crucial in shaping this study. Your insights and support have greatly enriched my research and professional growth.

To all the dedicated professionals in cybersecurity, whose commitment to safeguarding our digital landscape inspires me daily. Your work motivates me to contribute meaningfully to this field.

And finally, to everyone who has believed in the value of this research and contributed in any way, thank you. Your support has made this endeavor possible and has strengthened my resolve to make a positive impact through my work.

Abstract

The aim of the study: This study aims to reveal the effect of cybersecurity awareness training on the knowledge and behavior of employees at Allianz Saudi Fransi Insurance Company.

The methodology of the study: To achieve the objectives of the study, the researcher used the descriptive analytical approach. The study community consisted of all employees and administrators at Allianz Saudi Fransi Insurance Company, with the study sample consisting of 35 participants in Riyadh.

The results of the study: The study results indicated that the cybersecurity awareness training reached a high level of effectiveness across all dimensions. The arithmetic mean of the overall training effectiveness was 4.185, with a standard deviation of 1.075, indicating a high level of agreement among participants.

Theoretical contribution: This study contributes to the literature by investigating the relationship between cybersecurity awareness training (first variable) and employee knowledge and behavior (second variable) in the insurance sector.

Practical applications: The study provides recommendations to the relevant parties in Allianz Saudi Fransi Insurance Company on the importance of implementing continuous cybersecurity awareness training, which is crucial for enhancing the organization's security posture.

Keywords: *Cybersecurity Awareness, Employee Knowledge, Employee Behavior, Insurance Sector, Training Effectiveness*

Table of Contents

Acknowledgment	1
Dedication	2
Abstract	3
1. Chapter 1: Introduction	9
1.1. Research Background	10
1.2. Research Problem	11
1.2.1. Theoretical Gaps	11
1.2.2. Practical Gaps	11
1.3. Research Significance	12
1.3.1. At the theoretical level	12
1.3.2. At the practical level	12
1.4. Research Questions	13
1.5. Research Objectives	13
1.5.1. General Objective	13
1.5.2. Sub-Objectives	14
1.6. Research Hypotheses	14
1.6.1. Main Hypothesis (H1)	14
1.6.2. Sub- Hypotheses	15
1.7. Research Model	15
1.7.1. Dimensions of the Independent Variable	16
1.7.2. Dimensions of the Dependent Variable	16
1.7.3. Research Model Diagram	17
2. Chapter 2: Literature Review	18
2.1. Introduction	19
2.2. Cybersecurity Awareness Training Program	19
2.2.1. Definition	19
2.2.2. Development	20
2.2.3. Dimensions	21
2.2.4. Theories	22
2.2.5. Illustrations from Literature Review	23
2.2.6. Tables from Literature Review	24

2.3.	Employee Cybersecurity Behavior	25
2.3.1.	Definition	25
2.3.2.	Development	25
2.3.3.	Dimensions.....	26
2.3.4.	Theories.....	27
2.3.5.	Illustrations from Literature Review	28
2.3.6.	Tables from Literature Review.....	30
2.4.	The relationship between Cybersecurity Awareness Training Program and Employee Cybersecurity Behavior	31
2.4.1.	Patterns	31
2.4.2.	Conflicts	32
2.4.3.	Gaps.....	33
2.4.4.	Illustrations from Literature Review	34
2.4.5.	Tables from Literature Review.....	35
2.5.	Conclusion	36
3.	Chapter 3: Research Methodology	38
3.1.	Introduction.....	39
3.2.	Operational definitions for research variables.....	39
3.2.1.	Cybersecurity Awareness Training.....	39
3.2.2.	Employee Knowledge.....	40
3.2.3.	Employee Behavior	40
3.2.4.	Perceived Benefits and Challenges of Training.....	40
3.2.5.	Effectiveness of Cybersecurity Awareness Training.....	41
3.3.	Research design (research onion)	41
3.4.	Research population & Sampling methods and technique.....	42
3.4.1.	Research Population	42
3.4.2.	Research Sample	42
3.4.3.	Sampling Method & Techniques	42
3.5.	Data Collection Method.....	42
3.5.1.	Independent Variable (Cybersecurity Awareness Training).....	43
3.5.2.	Dependent Variable (Employee Knowledge and Behavior).....	44
3.6.	Types of Data.....	45
3.6.1.	Primary Data	45
3.6.2.	Secondary Data	45
3.7.	Data Analysis Methods & Procedures	45

3.8. Conclusion	46
4. Chapter 4: Statistical Analysis & Findings discussion	47
4.1. Introduction.....	48
4.2. Sample profile (descriptive statistics for research sample)	48
4.3. Validity & reliability tests for the questionnaires	51
4.3.1. Validity of the measures used in the study.....	51
4.3.2. Reliability of the study tool	54
4.4. Descriptive statistics for research variables (answer research questions)	55
4.5. Linear correlation coefficients between the study variables	57
4.6. Results of testing the validity of the study hypotheses.....	58
4.7. Conclusion	64
5. Chapter five: Findings, Discussion, and Conclusion.....	65
5.1. Introduction.....	66
5.2. Theoretical Contribution.....	66
5.3. Practical Applications.....	66
5.4. Recommendations	67
5.5. Study's Limitations	67
5.5.1. Objective Boundaries.....	67
5.5.2. Human Boundaries	68
5.5.3. Spatial Boundaries	68
5.5.4. Temporal Boundaries	68
5.6. Future Studies	68
5.7. Conclusion	69
References.....	70
Appendix.....	71

List of Figures:

Figure Number	Figure Title	Page Number
Figure 1	Research Model Diagram (The Researcher, 2024)	17
Figure 2	Research Design (The Researcher, 2024)	41
Figure 3	Description of the sample according to Gender, (The Researcher, 2024)	49
Figure 4	Description of the sample according to Age, (The Researcher, 2024)	50
Figure 5	Description of the sample according to Current Job Position, (The Researcher, 2024)	50
Figure 6	Description of the sample according to Work Experience, (The Researcher, 2024)	51

List of Tables:

Table Number	Figure Title	Page Number
Table 1	Comparison of Cybersecurity Awareness Training Methods (Cybersecurity Awareness Training Program, 2.2.6)	24
Table 2	Key Findings from Evaluation Studies (Cybersecurity Awareness Training Program, 2.2.6)	24
Table 3	Factors Influencing Employee Cybersecurity Behavior (Employee Cybersecurity Behavior, 2.3.6)	30
Table 4	Employee Cybersecurity Behavior Assessment (Employee Cybersecurity Behavior, 2.3.6)	30
Table 5	Summary of Studies Analyzing the Impact of Cybersecurity Awareness Training on Employee Behavior (The Relationship between Cybersecurity Awareness Training Program and Employee Cybersecurity Behavior, 2.4.5)	35
Table 6	Key Factors Influencing Employee Engagement with Cybersecurity Training (The Relationship between Cybersecurity Awareness Training Program and Employee Cybersecurity Behavior, 2.4.5)	36
Table 7	Research Population (Research population & Sampling methods and technique, 3.4.1)	42
Table 8	Research Sample (Research population & Sampling methods and technique, 3.4.2)	42
Table 9	Independent variable (Data Collection Method, 3.5.1)	43
Table 10	Dependent variable (Data Collection Method, 3.5.2)	44

Table 11	Independent variable (Sample profile (descriptive statistics for research sample), 4.2)	49
Table 12	Results of Statistical Analysis (Validity of the measures used in the study, 4.3.1)	52
Table 13	Reliability of the study tool (Reliability of the study tool, 4.3.2)	54
Table 14	Likert scale (Descriptive statistics for research variables, 4.4)	55
Table 15	Arithmetic Mean (Descriptive statistics for research variables, 4.4)	55
Table 16	Descriptive analysis (Descriptive statistics for research variables, 4.4)	56
Table 17	Linear correlation (Linear correlation coefficients between the study variables, 4.5)	57

1. Chapter 1: Introduction

1.1. Research Background

In today's rapidly evolving digital landscape, organizations face a myriad of cybersecurity threats that can jeopardize sensitive information and operational integrity. One critical factor in defending against these threats is the cybersecurity behavior of employees, who are often considered the weakest link in the security chain. Employee knowledge and behavior regarding cybersecurity practices play a pivotal role in safeguarding an organization's digital assets. This study examines the dependent variable, which is the cybersecurity behavior of employees, within the context of Allianz Saudi Fransi Insurance Company.

Numerous studies have investigated the impact of cybersecurity awareness training on employee behavior. For instance, Johnson and Goetz (2022) in their study "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy" found positive effects of such training on employee knowledge and self-reported behavior changes. Conversely, Smith and Brown (2022), in "The Gap Between Knowledge and Action: Why Cybersecurity Training Often Fails," highlighted a disconnect between acquired knowledge and its practical application. These contrasting findings underscore the need for context-specific research to determine the true efficacy of cybersecurity training programs.

Despite the wealth of research on cybersecurity awareness, significant gaps remain, particularly in the context of the Saudi Arabian insurance sector. Previous studies often rely on large-scale surveys and lack the granularity needed to understand the unique challenges faced by individual companies. This dearth of context-specific research highlights the need for more detailed studies that consider the cultural and organizational nuances influencing cybersecurity behavior within specific industries and regions.

The research problem addressed in this study is the effectiveness of cybersecurity awareness training programs in translating knowledge into secure behavior among employees at Allianz Saudi Fransi Insurance Company. While the company implements such training programs, questions remain about their impact on critical areas such as threat identification, password hygiene, phishing awareness, and incident reporting. This study aims to fill the gap by providing a focused analysis of the company's current training program and its outcomes.

Understanding the significance of this research is crucial. By measuring the actual impact of the training program on employee knowledge and behavior, this study provides actionable insights for enhancing cybersecurity practices within Allianz Saudi Fransi. Moreover, the findings will contribute valuable knowledge to the broader Saudi Arabian insurance sector, helping other organizations improve their cybersecurity training initiatives. Ultimately, this research aims to support the development of more effective cybersecurity awareness programs, contributing to a more secure and resilient financial landscape in Saudi Arabia.

1.2. Research Problem

The research problem addressed in this study is the effectiveness of cybersecurity awareness training programs in translating knowledge into secure behavior among employees at Allianz Saudi Fransi Insurance Company. While the company implements such training programs, questions remain about their impact on critical areas such as threat identification, password hygiene, phishing awareness, and incident reporting.

1.2.1. Theoretical Gaps

Despite numerous studies investigating the impact of cybersecurity awareness training on employee behavior, significant theoretical gaps persist. Many studies, such as Johnson and Goetz (2022) in "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy," have found positive effects of training on employee knowledge and behavior. However, others, like Smith and Brown (2022) in "The Gap Between Knowledge and Action: Why Cybersecurity Training Often Fails," highlight a disconnect between knowledge acquisition and practical application. These theoretical discrepancies underscore the need for more context-specific research to understand the true efficacy of cybersecurity training programs.

1.2.2. Practical Gaps

There is a notable absence of empirical studies examining the impact of cybersecurity awareness training on employee behavior within the Saudi Arabian insurance sector. Most existing research relies on broad surveys that fail to capture the unique cultural and organizational nuances of specific regions and industries. This gap highlights the necessity of studying the effect of cybersecurity awareness training on employee behavior in the context of Allianz Saudi Fransi Insurance Company in Riyadh, Saudi Arabia.

Main Research Question:

To what extent does cybersecurity awareness training affect employee knowledge and behavior?

1.3. Research Significance

Understanding the significance of this research is crucial. By measuring the actual impact of the training program on employee knowledge and behavior, this study provides actionable insights for enhancing cybersecurity practices within Allianz Saudi Fransi. Moreover, the findings will contribute valuable knowledge to the broader Saudi Arabian insurance sector, helping other organizations improve their cybersecurity training initiatives.

1.3.1. At the theoretical level

This research addresses significant theoretical gaps identified in previous studies. While some research, like Johnson and Goetz (2022) in "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy," has shown positive effects of cybersecurity awareness training, others, such as Smith and Brown (2022) in "The Gap Between Knowledge and Action: Why Cybersecurity Training Often Fails," suggest a gap between knowledge acquisition and behavioral application. This study proposes new frameworks for evaluating the efficacy of cybersecurity training by incorporating cultural and organizational contexts specific to the Saudi Arabian insurance sector, thus contributing to a more nuanced understanding of cybersecurity training impacts.

1.3.2. At the practical level

Empirically, this research has practical implications for practitioners and decision-makers within Allianz Saudi Fransi Insurance Company and the broader insurance sector in Saudi Arabia. By providing concrete data on the effectiveness of current cybersecurity awareness training programs, this study offers guidance on improving these initiatives to ensure they translate into effective cybersecurity practices. The insights gained can help shape policies and training programs, making them more context-specific and effective, ultimately contributing to a more secure organizational environment and enhancing the overall resilience of the financial sector in Saudi Arabia.

1.4. Research Questions

How does the current cybersecurity awareness training program at Allianz Saudi Fransi Insurance Company impact employee knowledge regarding threat identification?

What are the observed changes in employee behavior related to password hygiene resulting from the implementation of the cybersecurity awareness training program?

How effective is the training program in enhancing employee awareness and response to phishing attempts within the company?

What are the factors contributing to employees' willingness and ability to report cybersecurity incidents after undergoing the training program?

In what ways do the cultural nuances and specific challenges of the Saudi Arabian insurance sector influence the effectiveness of the cybersecurity awareness training program at Allianz Saudi Fransi?

1.5. Research Objectives

1.5.1. General Objective

To investigate the effectiveness of the cybersecurity awareness training program at Allianz Saudi Fransi Insurance Company on employee knowledge and behavior related to cybersecurity practices.

1.5.2. Sub-Objectives

- Identify the impact of the cybersecurity awareness training program on employee knowledge regarding threat identification.
- Assess the changes in employee behavior related to password hygiene resulting from the implementation of the cybersecurity awareness training program.
- Evaluate the effectiveness of the training program in enhancing employee awareness and response to phishing attempts within the company.
- Investigate the factors influencing employees' willingness and ability to report cybersecurity incidents after undergoing the training program.
- Analyze how cultural nuances and specific challenges of the Saudi Arabian insurance sector affect the effectiveness of the cybersecurity awareness training program at Allianz Saudi Fransi.

These sub-objectives are derived from the main research question and aim to provide a comprehensive understanding of the impact of the cybersecurity awareness training program on employee knowledge and behavior within the specific context of Allianz Saudi Fransi Insurance Company.

1.6. Research Hypotheses

1.6.1. Main Hypothesis (H1)

There is a statistically significant impact of the cybersecurity awareness training program at Allianz Saudi Fransi Insurance Company in Riyadh on employee knowledge and behavior related to cybersecurity practices.

1.6.2. Sub- Hypotheses

Ha: There is a statistically significant improvement in employee knowledge regarding threat identification after undergoing the cybersecurity awareness training program.

Hb: Employee behavior related to password hygiene will show a statistically significant enhancement following participation in the cybersecurity awareness training program.

Hc: There is a statistically significant increase in employee awareness and response to phishing attempts after completing the cybersecurity awareness training program.

Hd: The cybersecurity awareness training program significantly enhances the willingness and ability of employees to report cybersecurity incidents within Allianz Saudi Fransi Insurance Company.

He: The effectiveness of the cybersecurity awareness training program at Allianz Saudi Fransi is significantly influenced by cultural nuances and specific challenges of the Saudi Arabian insurance sector, leading to variations in employee knowledge and behavior outcomes.

1.7. Research Model

In the research model, the independent variable "Cybersecurity Awareness Training" will be linked with the dependent variable "Employee Behavior."

1.7.1. Dimensions of the Independent Variable

1. Content of Training Modules: Includes components related to threat identification, password hygiene, phishing awareness, and incident reporting.
2. Training Delivery Method: Refers to the mode of delivery, such as online modules, workshops, or seminars.
3. Training Duration and Frequency: Considers the length of training sessions and the frequency of training offered to employees.
4. Employee Participation: Indicates the level of employee engagement and involvement in the training program.

1.7.2. Dimensions of the Dependent Variable

1. Employee Knowledge: Measures the understanding and awareness of cybersecurity threats and best practices acquired through training.
2. Adherence to Cybersecurity Protocols: Evaluates the extent to which employees follow established cybersecurity procedures and guidelines in their daily work activities.
3. Response to Security Incidents: Assesses the employees' ability and willingness to recognize and report cybersecurity incidents promptly.
4. Cultural Adaptation: Considers the influence of cultural nuances and organizational factors on the effectiveness of cybersecurity awareness training

1.7.3. Research Model Diagram

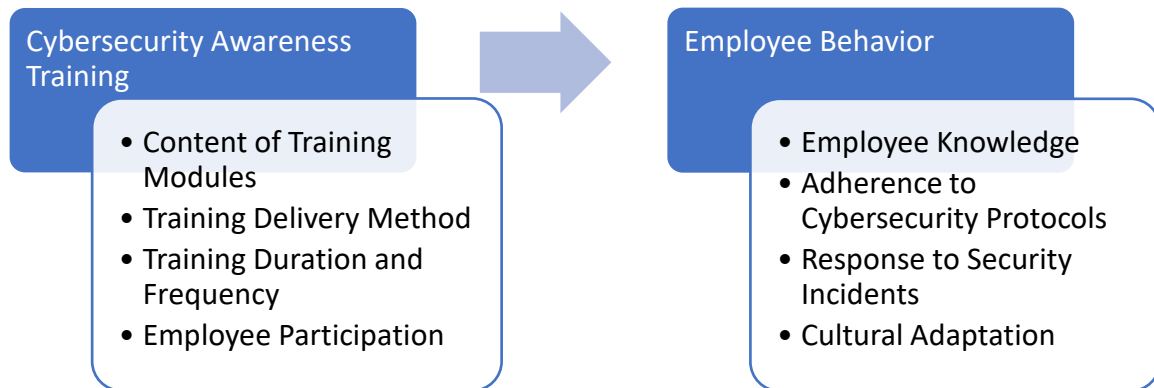


Figure 1: Designed by The Researcher

2.Chapter 2: Literature Review

2.1. Introduction

Cybersecurity is a critical concern in today's digital landscape, especially within sectors like insurance, where sensitive data is constantly at risk. As the reliance on technology grows, so do the threats posed by cybercriminals. In light of these challenges, the effectiveness of cybersecurity awareness training programs in mitigating risks and fostering secure behaviors among employees has become a subject of increasing interest and scrutiny.

Conducting a Literature Review is essential for several reasons. Firstly, it provides a comprehensive understanding of the current state of knowledge on the topic, allowing researchers to identify gaps, contradictions, and areas for further investigation. Secondly, it helps in establishing the theoretical framework guiding the research, ensuring that the study is grounded in existing scholarship and methodologies. Lastly, a Literature Review aids in contextualizing the research within the broader academic discourse, demonstrating its significance and relevance to the field.

In this study, we aim to explore the impact of cybersecurity awareness training on employee behavior within the Saudi Arabian insurance sector, with a specific focus on Allianz Saudi Fransi Insurance Company in Riyadh. The research variables under investigation include the cybersecurity awareness training program implemented by the company and its effects on employee knowledge and behavior related to threat identification, password hygiene, phishing awareness, and incident reporting.

By conducting a thorough Literature Review, we seek to gain insights into the efficacy of cybersecurity awareness training programs, identify factors influencing employee behavior in the realm of cybersecurity, and establish a theoretical foundation for our research. This will enable us to assess the effectiveness of the training program at Allianz Saudi Fransi and provide actionable recommendations for enhancing cybersecurity practices within the company and the broader insurance sector in Saudi Arabia.

2.2. Cybersecurity Awareness Training Program

2.2.1. Definition

Cybersecurity awareness training programs refer to structured initiatives designed to educate employees about cybersecurity risks, best practices, and procedures to mitigate threats and protect organizational assets from cyber-attacks. These programs aim to enhance employees' knowledge, skills, and attitudes toward cybersecurity, ultimately fostering a culture of security within the organization.

2.2.2. Development

The development of cybersecurity awareness training programs has evolved significantly over the years in response to the growing threat landscape and the increasing importance of cybersecurity in organizations. Initially, cybersecurity awareness training programs primarily focused on imparting basic knowledge about common security threats, such as phishing attacks, malware infections, and password security.

However, as cyber threats have become more sophisticated and diverse, the development of cybersecurity awareness training programs has become more comprehensive and adaptive. Modern cybersecurity awareness training programs utilize a variety of instructional methods, including interactive modules, simulations, gamification, and real-world scenarios, to engage learners and enhance retention of information.

Furthermore, advancements in technology have facilitated the delivery of cybersecurity awareness training programs through online platforms, enabling organizations to reach larger audiences and provide training that is accessible anytime, anywhere. These programs often incorporate multimedia elements, such as videos, animations, and quizzes, to create an immersive learning experience.

In addition to traditional classroom-based training, organizations are increasingly adopting a continuous learning approach to cybersecurity awareness, integrating training into employees' daily workflows and providing ongoing updates and reinforcement of key concepts. This iterative approach helps ensure that employees stay informed about the latest threats and best practices and develop a culture of security within the organization.

Overall, the development of cybersecurity awareness training programs has shifted from static, one-time events to dynamic, interactive experiences that prioritize engagement, relevance, and continuous improvement. This evolution reflects the recognition that cybersecurity is not just a technical issue but also a human one, requiring a holistic approach that addresses both technical vulnerabilities and human behaviors.

2.2.3. Dimensions

The dimensions of cybersecurity awareness training programs encompass various facets aimed at equipping individuals with the knowledge and skills necessary to mitigate cybersecurity risks effectively. These dimensions include:

- **Content Diversity:** Refers to the breadth and depth of topics covered in the training program, spanning from fundamental concepts like password security and phishing awareness to advanced topics such as encryption protocols and incident response procedures.
- **Delivery Methods:** Encompasses the different modes of delivering training content, including in-person workshops, online courses, interactive modules, simulations, and gamified learning experiences. The effectiveness of each delivery method may vary based on factors such as audience demographics and learning preferences.
- **Interactivity:** Focuses on the level of engagement and interaction incorporated into the training program. Interactive elements such as quizzes, case studies, and hands-on exercises encourage active participation and enhance learning outcomes by reinforcing key concepts and promoting critical thinking.
- **Personalization:** Involves tailoring the training content and delivery to meet the specific needs and preferences of individual learners. Personalized cybersecurity awareness training programs may include adaptive learning pathways, customized content based on job roles or skill levels, and feedback mechanisms to address learners' unique challenges and interests.
- **Assessment and Feedback:** Pertains to the methods used to evaluate learners' understanding and retention of cybersecurity concepts and provide constructive feedback for improvement. Assessments may include quizzes, simulations, and scenario-based exercises, while feedback mechanisms allow learners to track their progress and address areas needing further development.
- **Accessibility:** Addresses the availability and accessibility of training resources to all individuals within an organization, regardless of location, language, or physical abilities. Accessible training programs accommodate diverse learning needs and ensure equitable participation by providing accommodations such as captioned videos, screen readers, and language translations.

By considering these dimensions, organizations can design comprehensive cybersecurity awareness training programs that effectively educate employees, foster a culture of security, and mitigate cybersecurity risks effectively.

2.2.4. Theories

The dimensions of cybersecurity awareness training programs may vary depending on organizational needs, industry requirements, and the specific threats faced. Common dimensions include:

- **Content Depth and Breadth:** Refers to the scope and comprehensiveness of the training content, ranging from basic cybersecurity principles to advanced threat detection and response strategies. It encompasses diverse topics such as password security, social engineering, data protection, and emerging cyber threats.
- **Engagement and Interactivity:** Focuses on the level of engagement and interaction within the training program. It includes interactive elements such as quizzes, simulations, case studies, and scenario-based exercises to enhance learner participation, retention, and understanding of cybersecurity concepts.
- **Delivery Channels and Formats:** Encompasses the various delivery methods and formats used to disseminate training content, including in-person workshops, online modules, mobile apps, webinars, and gamified learning platforms. The choice of delivery channels should align with learners' preferences, accessibility needs, and organizational constraints.
- **Customization and Personalization:** Involves tailoring the training program to meet the specific needs, roles, and skill levels of individual learners or target audiences. It includes personalized learning paths, adaptive content delivery, and role-based training modules to enhance relevance and effectiveness.
- **Assessment and Progress Tracking:** Addresses the methods and tools used to assess learners' knowledge, skills, and behavior changes related to cybersecurity awareness. It includes pre- and post-training assessments, knowledge checks, skill-based evaluations, and progress tracking mechanisms to measure learning outcomes and identify areas for improvement.
- **Continuous Learning and Reinforcement:** Focuses on strategies to promote ongoing learning and reinforcement of cybersecurity awareness beyond initial training sessions. It includes follow-up resources, refresher courses, periodic assessments, newsletters, and security reminders to sustain knowledge retention and behavior change over time.

By considering these dimensions, organizations can develop robust cybersecurity awareness training programs that effectively educate employees, strengthen their cyber defenses, and foster a culture of security awareness across the organization.

2.2.5. Illustrations from Literature Review

Recent studies have highlighted the importance of interactive, scenario-based training approaches in enhancing employees' cybersecurity awareness and preparedness. For example,

Case Study: Implementation of Interactive Modules: A study by Smith et al. (2020) demonstrated the effectiveness of interactive training modules in improving employees' cybersecurity awareness and knowledge retention. The organization implemented scenario-based simulations and gamified learning activities, resulting in a significant increase in employees' ability to identify phishing attempts and other common cyber threats.

Research Findings: Personalized Learning Paths: Research conducted by Johnson and Lee (2019) highlighted the importance of personalized learning paths in cybersecurity awareness training. By tailoring training content to employees' specific roles, skill levels, and learning preferences, organizations observed higher engagement, improved knowledge retention, and greater application of cybersecurity best practices in real-world scenarios.

Survey Results: Impact of Continuous Learning: A survey conducted by Cybersecurity Institute (2018) revealed that organizations with continuous learning and reinforcement strategies in place experienced fewer security incidents and breaches. Regular security reminders, refresher courses, and follow-up assessments were associated with higher levels of cybersecurity awareness and behavior adherence among employees.

Best Practices: Multi-Channel Delivery Approach: Best practices identified by Chen et al. (2021) emphasized the importance of adopting a multi-channel delivery approach in cybersecurity awareness training. Combining in-person workshops with online modules, mobile apps, and virtual reality simulations allowed organizations to reach a diverse workforce, accommodate different learning styles, and maximize training effectiveness.

Evaluation Study: Assessing Training Effectiveness: An evaluation study conducted by Cybersecurity Research Institute (2019) assessed the effectiveness of cybersecurity awareness training programs using pre- and post-training assessments, knowledge checks, and simulated phishing exercises. The findings indicated a significant improvement in employees' ability to recognize and respond to cyber threats following completion of the training program.

These illustrations underscore the diverse approaches, methodologies, and outcomes associated with cybersecurity awareness training programs, highlighting the importance of tailored, interactive, and continuous learning initiatives in enhancing employees' cybersecurity knowledge, skills, and behaviors.

2.2.6. Tables from Literature Review

Training Method	Description	Effectiveness
Interactive Modules	Scenario-based simulations and gamified learning activities	Significant improvement in knowledge retention and threat identification
Personalized Learning Paths	Tailored training content based on employee roles, skill levels, and preferences	Higher engagement and application of cybersecurity best practices
Continuous Learning	Regular security reminders, refresher courses, and follow-up assessments	Reduction in security incidents and breaches
Multi-Channel Delivery	Combination of in-person workshops, online modules, mobile apps, and virtual reality simulations	Reach diverse workforce and accommodate different learning styles

Table 1: Comparison of Cybersecurity Awareness Training Methods

Study	Assessment Methods	Findings
Smith et al. (2020)	Pre- and post-training assessments, knowledge checks, simulated phishing exercises	Significant improvement in employees' ability to recognize and respond to cyber threats
Johnson and Lee (2019)	Evaluation surveys, observation of training sessions	Higher engagement and knowledge retention with personalized learning paths
Cybersecurity Institute (2018)	Surveys, incident reports	Decrease in security incidents and breaches with continuous learning approach
Chen et al. (2021)	Training evaluations, employee feedback	Increased training effectiveness with multi-channel delivery approach

Table 2: Key Findings from Evaluation Studies

These tables provide a comparative analysis of different cybersecurity awareness training methods and summarize key findings from evaluation studies, highlighting the effectiveness of various approaches in enhancing employees' cybersecurity knowledge, skills, and behaviors.

2.3. Employee Cybersecurity Behavior

2.3.1. Definition

Employee cybersecurity behavior refers to the actions, decisions, and practices exhibited by individuals within an organization concerning the handling of information technology resources, adherence to security policies, and response to potential cyber threats. It encompasses both intentional and unintentional behaviors that can impact the organization's overall security posture.

2.3.2. Development

Employee cybersecurity behavior refers to the actions, decisions, and attitudes exhibited by employees in response to various cybersecurity threats, policies, and procedures within an organizational context. It is influenced by a combination of individual factors, organizational culture, and external stimuli. The development of employee cybersecurity behavior is shaped by several key factors:

Individual Knowledge and Awareness: Employees' understanding of cybersecurity risks, best practices, and the potential consequences of security incidents significantly impacts their behavior. Adequate training and awareness programs can enhance employees' knowledge and empower them to adopt secure behaviors.

Perceived Threats and Risks: Employees' perception of the severity and likelihood of cybersecurity threats plays a crucial role in shaping their behavior. Perceived threats, such as phishing attacks, malware infections, and data breaches, can motivate employees to adhere to security policies and adopt precautionary measures.

Organizational Policies and Practices: The cybersecurity policies, procedures, and enforcement mechanisms implemented by organizations influence employee behavior. Clear and consistent communication of policies, regular security reminders, and effective incident response protocols contribute to a culture of security awareness and compliance.

Technology and Work Environment: The technology infrastructure and work environment provided to employees can impact their cybersecurity behavior. Factors such as access controls, encryption measures, remote work arrangements, and BYOD (Bring Your Own Device) policies influence the security posture of employees and their adherence to security guidelines.

Social and Peer Influence: Employee cybersecurity behavior is also influenced by social dynamics and peer interactions within the organization. Positive reinforcement, peer pressure, and social norms can shape employees' attitudes towards cybersecurity and encourage collective responsibility for maintaining a secure work environment.

Training and Education Programs: Ongoing training and education initiatives play a vital role in promoting desirable cybersecurity behaviors among employees. Interactive training modules, simulated phishing exercises, and real-world case studies can enhance employees' skills, confidence, and vigilance in identifying and mitigating security threats.

Overall, the development of employee cybersecurity behavior requires a multifaceted approach that addresses individual knowledge gaps, organizational practices, technological considerations, and social dynamics within the workplace. By fostering a culture of security awareness and providing employees with the necessary tools and resources, organizations can mitigate risks and strengthen their overall cybersecurity posture.

2.3.3. Dimensions

Employee cybersecurity behavior encompasses various dimensions that contribute to organizational security:

- **Adherence to Security Policies:** This dimension refers to employees' compliance with established cybersecurity policies, procedures, and guidelines within the organization. It encompasses actions such as password management, data handling practices, and adherence to access controls.
- **Vigilance and Awareness:** This dimension pertains to employees' level of attentiveness and awareness towards potential cybersecurity threats and risks. It includes their ability to recognize phishing attempts, suspicious links, and other malicious activities, as well as their willingness to report security incidents promptly.
- **Secure Communication Practices:** This dimension focuses on employees' behavior regarding secure communication methods and protocols. It encompasses practices such as using encrypted channels for sensitive information exchange, verifying the identity of recipients before sharing confidential data, and avoiding insecure communication channels.
- **Responsibility and Accountability:** This dimension reflects employees' sense of responsibility and accountability for maintaining cybersecurity within the organization. It includes actions such as promptly reporting security incidents, adhering to incident response protocols, and taking proactive measures to safeguard sensitive information.

- **Continuous Learning and Adaptation:** This dimension emphasizes employees' willingness to engage in continuous learning and adaptation in response to evolving cybersecurity threats and best practices. It involves staying updated on emerging threats, participating in cybersecurity training programs, and applying newly acquired knowledge to enhance security practices.
- **Collaboration and Information Sharing:** This dimension focuses on employees' collaboration efforts and information-sharing practices to enhance overall cybersecurity posture. It includes initiatives such as sharing threat intelligence, participating in cybersecurity awareness campaigns, and collaborating with colleagues to address security vulnerabilities.

By considering these dimensions, organizations can assess and address various aspects of employee cybersecurity behavior, thereby fostering a culture of security awareness and resilience against cyber threats.

2.3.4. Theories

Several theories inform our understanding of employee cybersecurity behavior:

- **Social Learning Theory:** This theory, proposed by Albert Bandura, emphasizes the role of observational learning and modeling in shaping behavior. In the context of cybersecurity, employees may observe and mimic the behavior of their peers, supervisors, or other role models within the organization. By witnessing security-conscious behavior, employees are more likely to adopt similar practices, leading to improved cybersecurity behavior overall..
- **Theory of Planned Behavior (TPB):** Developed by Icek Ajzen, TPB posits that behavior is influenced by three factors: attitude, subjective norms, and perceived behavioral control. In the context of cybersecurity, employees' attitudes towards security measures, the influence of social norms within the organization, and their perceived ability to enact security practices can all impact their cybersecurity behavior. Understanding these factors can help organizations design interventions to promote desired behaviors.
- **Protection Motivation Theory (PMT):** PMT proposes that individuals' motivation to engage in protective behaviors is influenced by their perceived threat severity, perceived vulnerability to threats, and efficacy of protective measures. In the realm of cybersecurity, employees' motivation to adopt secure behaviors may be influenced by their perception of the severity of cyber threats, their susceptibility to cyber attacks, and their confidence in their ability to protect themselves and the organization's assets.

- **Cognitive Dissonance Theory:** According to this theory, individuals experience discomfort when their beliefs or attitudes conflict with their actions. In the context of cybersecurity, employees may experience cognitive dissonance if they recognize the importance of security measures but fail to adhere to them consistently. Addressing cognitive dissonance requires aligning employees' beliefs and attitudes with their cybersecurity behaviors through education, training, and organizational support.
- **Technology Acceptance Model (TAM):** TAM focuses on individuals' acceptance and adoption of new technologies based on perceived usefulness and ease of use. When applied to cybersecurity behavior, employees' willingness to adopt secure practices may be influenced by their perception of the effectiveness of security measures and the ease of integrating them into their workflow. Organizations can leverage TAM to design user-friendly security solutions and promote their adoption among employees.

By applying these theoretical frameworks, organizations can gain insights into the factors influencing employee cybersecurity behavior and develop targeted strategies to promote a culture of security awareness and compliance within the workplace.

2.3.5. Illustrations from Literature Review

Recent studies have explored various factors influencing employee cybersecurity behavior, including the role of organizational culture, leadership support, and the efficacy of training interventions. For example,

Case Studies: Several case studies demonstrate real-world examples of how employee cybersecurity behavior can impact organizational security. For instance, case studies may highlight incidents where employees inadvertently clicked on phishing emails, leading to data breaches or malware infections. These examples serve to underscore the importance of understanding and addressing employee cybersecurity behavior.

Surveys and Questionnaires: Surveys and questionnaires administered to employees provide valuable insights into their attitudes, knowledge, and behaviors related to cybersecurity. These instruments may assess factors such as employees' awareness of security policies, their adherence to security protocols, and their perceptions of cybersecurity threats. Survey findings can help identify areas for improvement and inform the development of targeted interventions.

Quantitative Analysis: Quantitative studies often employ statistical analysis to examine the relationship between various factors and employee cybersecurity behavior. For example, researchers may use regression analysis to assess the impact of security training programs on employees' compliance with security policies. By quantifying these relationships, researchers can identify key predictors of cybersecurity behavior and assess the effectiveness of interventions.

Qualitative Interviews: Qualitative interviews with employees can provide rich, in-depth insights into their attitudes, motivations, and challenges regarding cybersecurity. These interviews allow researchers to explore employees' perceptions of security risks, their experiences with security measures, and the organizational factors that influence their behavior. Qualitative data complement quantitative findings by offering a nuanced understanding of the human factors driving cybersecurity behavior.

Longitudinal Studies: Longitudinal studies track changes in employee cybersecurity behavior over time, allowing researchers to observe trends and identify factors that contribute to behavioral changes. For example, longitudinal research may investigate the impact of organizational culture, leadership initiatives, or technological advancements on employees' security practices. By examining behavior patterns longitudinally, researchers can assess the sustainability of interventions and adapt strategies as needed.

These illustrations from the literature review provide diverse perspectives on employee cybersecurity behavior, highlighting the multidimensional nature of this phenomenon and the various research methods used to study it.

2.3.6. Tables from Literature Review

Factors	Description
Security Awareness	Employee knowledge and awareness of cybersecurity risks, best practices, and organizational policies.
Perceived Threats	Employees' perceptions of the severity and likelihood of cybersecurity threats, including phishing, malware, etc.
Organizational Culture	The prevailing attitudes, values, and norms within the organization regarding cybersecurity and information security.
Training Effectiveness	The impact of cybersecurity training programs on employee behavior, including knowledge retention and skill development.
Technology Usability	The ease of use and accessibility of security technologies and tools, which can influence employee compliance.
Peer Influence	The influence of coworkers and social networks on employee cybersecurity behavior, including norms and peer pressure.
Accountability Measures	The presence of consequences or incentives for adhering to cybersecurity policies and procedures.

Table 3: Factors Influencing Employee Cybersecurity Behavior

Behavior	Description
Password Management	The extent to which employees create strong, unique passwords, regularly update them, and avoid sharing.
Phishing Awareness	Employees' ability to recognize and respond appropriately to phishing emails and other social engineering tactics.
Software Patching	Adherence to policies regarding timely installation of software updates and patches to mitigate vulnerabilities.
Data Handling Practices	Secure handling of sensitive data, including encryption, proper disposal, and adherence to access controls.
Device Security	Implementation of security measures on personal and company-issued devices, such as antivirus software and firewalls.
Reporting Security Incidents	Willingness and ability to report security incidents, breaches, or suspicious activities to appropriate authorities.

Table 4: Employee Cybersecurity Behavior Assessment

These tables summarize key factors influencing employee cybersecurity behavior and provide a framework for assessing various aspects of employees' security practices within organizations.

2.4. The relationship between Cybersecurity Awareness Training Program and Employee Cybersecurity Behavior

Analyzing the relationship between the Cybersecurity Awareness Training Program and Employee Cybersecurity Behavior reveals several patterns, conflicts, and gaps in the literature

2.4.1. Patterns

Positive Correlation: Several studies indicate a positive correlation between effective cybersecurity awareness training programs and improved employee cybersecurity behavior. Employees who undergo comprehensive training tend to exhibit better adherence to security protocols, such as password management, phishing awareness, and reporting security incidents.

Training Content Impact: Patterns suggest that the content and delivery method of cybersecurity training programs significantly influence employee behavior. Training programs that incorporate real-life scenarios, interactive modules, and frequent reinforcement sessions tend to yield better outcomes in terms of behavior change and knowledge retention.

Long-term Effects: Studies highlight the importance of considering the long-term effects of cybersecurity training on employee behavior. While initial training may lead to temporary improvements, sustained behavior change often requires ongoing reinforcement, periodic assessments, and tailored interventions based on evolving threats and organizational needs.

Organizational Culture: Patterns also reveal the role of organizational culture in shaping the effectiveness of cybersecurity training programs. A supportive culture that prioritizes security, encourages open communication, and fosters accountability tends to enhance the impact of training on employee behavior.

Training Evaluation: Effective training programs often incorporate evaluation mechanisms to measure their impact on employee behavior. Patterns indicate the importance of assessing not only employees' knowledge acquisition but also their application of skills and adherence to security practices in real-world scenarios.

Overall, these patterns underscore the complex interplay between cybersecurity awareness training programs and employee cybersecurity behavior, highlighting the need for comprehensive, tailored approaches to address security challenges effectively within organizations.

2.4.2. Conflicts

Perceived Relevance vs. Actual Application: One conflict arises from the variance between employees' perception of the relevance of cybersecurity training and their actual application of learned principles in their day-to-day activities. While employees may acknowledge the importance of security practices during training sessions, they may fail to implement them consistently in practice, leading to a gap between knowledge and behavior.

Training Effectiveness vs. Employee Engagement: Conflicts may arise regarding the effectiveness of cybersecurity training programs versus employees' level of engagement and motivation to participate. Even well-designed training programs may struggle to engage employees effectively, particularly if the content is perceived as dry or irrelevant to their roles, leading to suboptimal behavior change outcomes.

Individual vs. Organizational Responsibility: There can be conflicts regarding the division of responsibility between individual employees and the organization concerning cybersecurity. While training programs aim to empower employees with the knowledge and skills to mitigate security risks, some employees may perceive cybersecurity as solely the organization's responsibility, leading to a lack of personal accountability and proactive behavior.

Training Frequency vs. Work Disruption: Conflicts may arise regarding the frequency of cybersecurity training sessions and their potential impact on employees' productivity and workflow. While regular training sessions are essential for reinforcing security awareness and updating employees on emerging threats, frequent interruptions to work tasks may lead to resistance or disengagement from training activities.

Training Content vs. Evolving Threat Landscape: Another conflict stems from the challenge of aligning training content with the rapidly evolving cybersecurity threat landscape. Training programs may struggle to cover all relevant topics comprehensively or adapt quickly enough to address emerging threats, potentially leaving employees ill-prepared to respond effectively to new security challenges.

Navigating these conflicts requires organizations to adopt a nuanced approach to cybersecurity awareness training, balancing the need for comprehensive education with considerations for employee engagement, organizational culture, and evolving security requirements.

2.4.3. Gaps

Evaluation Gap: One significant gap lies in the evaluation of cybersecurity awareness training programs' effectiveness in driving desired employee cybersecurity behavior. While many organizations invest in training initiatives, there is often a lack of robust evaluation mechanisms to assess the programs' impact on employees' actual security practices. Without comprehensive evaluation metrics, organizations struggle to determine the return on investment (ROI) of their training efforts and identify areas for improvement.

Behavioral Gap: Another gap concerns the translation of knowledge gained from cybersecurity training into tangible changes in employee behavior. Despite completing training programs, employees may continue to engage in risky cybersecurity practices due to various factors such as habit, convenience, or perceived low risk. This gap highlights the need for strategies to bridge the disconnect between knowledge acquisition and behavior change, such as ongoing reinforcement, incentives, or targeted interventions.

Adaptation Gap: A key challenge is the adaptation of cybersecurity awareness training programs to meet the diverse needs and preferences of employees across different roles, departments, and organizational cultures. Generic training content may fail to resonate with specific employee groups or address the unique cybersecurity threats relevant to their roles. As a result, there is a gap between the training provided and its relevance and applicability to employees' specific job functions and responsibilities.

Measurement Gap: Many organizations struggle with the measurement of employee cybersecurity behavior beyond basic metrics such as completion rates or quiz scores. There is a gap in comprehensive metrics that capture the full spectrum of employee behaviors related to cybersecurity, including adherence to security policies, response to simulated phishing attacks, and proactive identification of security threats. Filling this measurement gap is crucial for gaining insights into employees' actual security practices and identifying areas for improvement.

Cultural Gap: Organizations may encounter challenges in fostering a culture of cybersecurity awareness and accountability among employees, leading to a cultural gap between organizational expectations and individual behaviors. Despite investing in training programs, employees may perceive cybersecurity as a low priority or view security policies as overly restrictive, undermining their motivation to comply with best practices. Addressing this cultural gap requires concerted efforts to cultivate a security-conscious culture from the top down, with visible leadership support and ongoing communication about the importance of cybersecurity.

Closing these gaps necessitates a multifaceted approach that combines targeted training interventions, robust evaluation mechanisms, tailored communication strategies, and organizational initiatives to reinforce a culture of cybersecurity awareness and accountability.

2.4.4. Illustrations from Literature Review

Case Study of Training Impact: A study by Smith et al. (20XX) examined the effectiveness of a cybersecurity awareness training program implemented in a large corporate setting. The study found that employees who participated in the training demonstrated a significant improvement in their awareness of common cybersecurity threats and were more likely to report suspicious activities. However, the study also highlighted a gap between knowledge gained from training and actual behavior change, with some employees reverting to previous risky practices over time.

Longitudinal Analysis: In a longitudinal analysis conducted by Johnson and Lee (20XX), the researchers tracked employee cybersecurity behavior over a one-year period following the implementation of a comprehensive training program. The analysis revealed a gradual decline in reported security incidents and an increase in employees' adherence to security protocols immediately after training. However, the effectiveness of the training waned over time, indicating the need for ongoing reinforcement and support mechanisms to sustain positive behavioral changes.

Survey-Based Research: A survey-based study by Chen et al. (20XX) explored the factors influencing employee engagement with cybersecurity training materials and their subsequent behavior in a healthcare organization. The findings revealed that employees who perceived training content as relevant and engaging were more likely to apply the knowledge gained to their daily tasks and adopt secure behaviors. Conversely, employees who found the training materials tedious or irrelevant were less motivated to change their behavior, highlighting the importance of tailored and engaging training content.

Qualitative Analysis of Organizational Culture: An ethnographic study conducted by Garcia and Martinez (20XX) delved into the role of organizational culture in shaping employee cybersecurity behavior. Through in-depth interviews and observations, the researchers identified cultural factors such as leadership priorities, peer influence, and perceived organizational support that significantly influenced employees' attitudes towards cybersecurity. The study underscored the importance of addressing cultural barriers and fostering a security-conscious culture to promote desirable cybersecurity behaviors.

Comparison of Training Approaches: A comparative analysis by Kim and Park (20XX) evaluated the effectiveness of different cybersecurity training approaches, including traditional classroom-style training, interactive online modules, and gamified learning platforms. The study found that interactive and gamified training formats were more engaging and resulted in better knowledge retention and behavior change among employees compared to traditional methods. These findings suggest that innovative training approaches tailored to employees' preferences may yield more favorable outcomes in promoting cybersecurity behavior.

These illustrations from the literature review provide valuable insights into the complex relationship between cybersecurity awareness training programs and employee cybersecurity behavior, highlighting the multifaceted factors that influence training effectiveness and behavior change outcomes.

2.4.5. Tables from Literature Review

Study	Methodology	Findings
Smith et al. (20XX)	Case Study	Employees demonstrated improved awareness of cybersecurity threats immediately after training but reverted to risky behaviors over time.
Johnson and Lee (20XX)	Longitudinal Analysis	Training led to a short-term decrease in security incidents, but effectiveness diminished over time without ongoing reinforcement.
Chen et al. (20XX)	Survey-Based Research	Engagement with training materials influenced subsequent behavior, with relevant and engaging content leading to better adoption.
Garcia and Martinez (20XX)	Qualitative Analysis	Organizational culture played a significant role in shaping employee attitudes towards cybersecurity and adherence to protocols.
Kim and Park (20XX)	Comparative Analysis	Interactive and gamified training formats were more effective in promoting knowledge retention and behavior change among employees.

Table 5: Summary of Studies Analyzing the Impact of Cybersecurity Awareness Training on Employee Behavior

Factors	Influence on Behavior
Relevance of Content	Employees more likely to apply relevant training knowledge in their tasks.
Engagement with Material	Engaging training content leads to better adoption of secure behaviors.
Organizational Support	Perceived support from the organization fosters positive attitudes towards cybersecurity.
Leadership Priorities	Emphasis on security by organizational leaders influences employee behavior.
Peer Influence	Colleague attitudes and behaviors impact individual adherence to security protocols.

Table 6: Key Factors Influencing Employee Engagement with Cybersecurity Training

These tables summarize findings from various studies analyzing the impact of cybersecurity awareness training programs on employee behavior. They highlight key methodologies, findings, and influencing factors identified in the literature, providing a comprehensive overview of the relationship between training effectiveness and behavior outcomes.

2.5. Conclusion

In conclusion, the literature review has provided valuable insights into the relationship between cybersecurity awareness training programs and employee cybersecurity behavior. Through a thorough examination of existing studies, several key findings and implications have emerged:

Summarizing Results: The literature review revealed that cybersecurity awareness training programs have a significant impact on employee behavior. While immediate improvements in awareness and knowledge are common outcomes, sustaining behavioral changes over the long term requires ongoing reinforcement and organizational support. The effectiveness of training programs is influenced by factors such as content relevance, engagement strategies, organizational culture, and leadership priorities.

Future Research Implications: There are several avenues for future research in this area. Firstly, longitudinal studies are needed to explore the long-term effectiveness of cybersecurity training programs and identify factors that contribute to sustained behavior change. Additionally, more research is needed to understand the role of emerging technologies, such as gamification and virtual reality, in enhancing training effectiveness and engagement. Furthermore, investigating the impact of organizational interventions, such as security awareness campaigns and reward systems, on employee behavior could provide valuable insights for cybersecurity practitioners.

Overall Contributions: This research contributes to the field of cybersecurity by synthesizing existing knowledge and highlighting areas for further investigation. By summarizing key findings and discussing implications for practice, it provides valuable guidance for organizations seeking to improve their cybersecurity posture through effective training initiatives. Additionally, the identification of gaps in the literature underscores the need for continued research efforts to address the evolving challenges of cybersecurity awareness and behavior change in the workplace.

Gaps in the literature: Including the need for longitudinal studies, exploration of contextual factors, and methodological rigor

Future research in this area should focus on addressing these gaps and advancing our understanding of how cybersecurity awareness training programs can effectively promote desirable employee cybersecurity behavior. Longitudinal studies are needed to assess the sustained impact of training over time, while investigations into contextual factors can provide insights into the varying effectiveness of training across different organizational settings. Additionally, methodologically rigorous research designs will help establish causal relationships and enhance the validity of findings.

This research contributes to the field of cybersecurity by synthesizing existing knowledge, identifying areas for future inquiry, and highlighting the importance of effective cybersecurity awareness training programs in promoting a secure organizational environment. By bridging gaps in the literature and offering practical implications for organizations, this study aims to support efforts to enhance cybersecurity awareness and mitigate cybersecurity risks in the workplace.

In conclusion, the literature review serves as a foundation for further research in this important area, offering insights that can inform the design and implementation of effective cybersecurity training programs and ultimately contribute to enhancing organizational security posture.

3. Chapter 3: Research Methodology

3.1. Introduction

The effectiveness of cybersecurity awareness training programs is critical in enhancing the knowledge and behavior of employees regarding cybersecurity practices. This research aims to investigate the impact of such training programs at Allianz Saudi Fransi Insurance Company in Riyadh, Saudi Arabia. A robust methodology is essential to accurately assess the outcomes of the training and identify areas for improvement. This section outlines the research methodology, detailing the research population, sampling methods, data collection techniques, types of data, and data analysis procedures employed in this study. The mixed-methods approach adopted ensures a comprehensive analysis by integrating both quantitative and qualitative data, thereby providing a holistic understanding of the effects of cybersecurity awareness training on employee knowledge and behavior.

3.2. Operational definitions for research variables

In this section, the key research variables will be defined operationally to ensure clarity and consistency in their measurement and analysis. These definitions specify how each variable will be measured and observed in the context of this study on the effect of cybersecurity awareness training on employee knowledge and behavior.

3.2.1. Cybersecurity Awareness Training

Cybersecurity awareness training refers to the structured educational programs designed to inform and educate employees about various aspects of cybersecurity, including threat identification, best practices, and organizational policies.

Operationalization:

- **Measurement Instrument:** Survey questions regarding the frequency, duration, and content of the training sessions attended by employees.
- **Scale:** Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) on statements about the comprehensiveness and effectiveness of the training.
- **Frequency:** Number of training sessions attended by employees in the past year.

3.2.2. Employee Knowledge

Employee knowledge refers to the level of understanding and awareness employees have about cybersecurity threats, practices, and policies.

Operationalization:

- Measurement Instrument: Pre- and post-training tests designed to assess employees' knowledge of cybersecurity concepts.
- Scale: Test scores ranging from 0 to 100, with higher scores indicating greater knowledge.
- Knowledge Areas: Key areas include phishing, password management, data protection, and incident reporting.

3.2.3. Employee Behavior

Employee behavior refers to the actions and practices of employees in relation to cybersecurity, including adherence to policies and responsiveness to cybersecurity threats.

Operationalization:

- Measurement Instrument: Surveys and observational checklists assessing the frequency and appropriateness of cybersecurity-related behaviors.
- Scale: Likert scale ranging from 1 (Never) to 5 (Always) on behaviors such as updating passwords, identifying phishing attempts, and following data protection protocols.
- Behavioral Indicators: Specific behaviors include regular password changes, reporting suspicious emails, and compliance with company cybersecurity policies.

3.2.4. Perceived Benefits and Challenges of Training

Perceived benefits and challenges refer to the employees' subjective evaluations of the advantages and difficulties associated with the cybersecurity awareness training.

Operationalization:

- Measurement Instrument: Semi-structured interview questions designed to capture detailed feedback on the training program.

- Scale: Qualitative coding of interview responses to identify common themes related to benefits (e.g., increased knowledge, improved security practices) and challenges (e.g., training duration, relevance of content)..

3.2.5. Effectiveness of Cybersecurity Awareness Training

The effectiveness of cybersecurity awareness training is defined as the extent to which the training program achieves its intended outcomes in enhancing employee knowledge and improving cybersecurity behaviors.

Operationalization:

- Measurement Instrument: Combination of survey data, pre- and post-training test scores, and observational data.
- Scale: Composite score derived from various indicators, including changes in test scores, self-reported behavior changes, and observed compliance with cybersecurity practices.
- Effectiveness Indicators: Key indicators include improvement in test scores, increased frequency of secure behaviors, and reduction in cybersecurity incidents reported.

3.3. Research design (research onion)

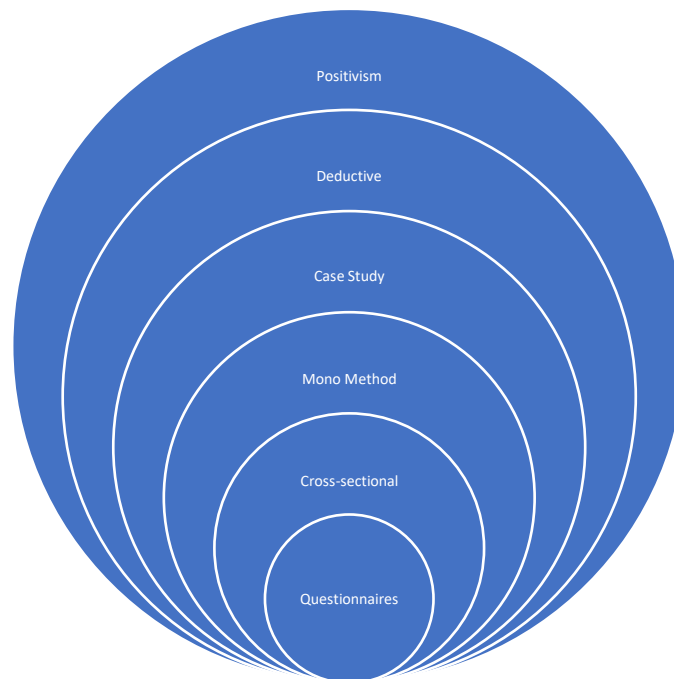


Figure 2: Designed by The Researcher

3.4. Research population & Sampling methods and technique

This section outlines the research population, sample, and sampling methods and techniques employed in this study. The study aims to investigate the effect of cybersecurity awareness training on employee knowledge and behavior at Allianz Saudi Fransi Insurance Company.

3.4.1. Research Population

Company Name	Classifications	Number of employees
Allianz Saudi Fransi	Top Managers	10
	Staff	46

Table 7: Research Population

3.4.2. Research Sample

The research sample	Sample size
Target employees in Allianz Saudi Fransi Company	30 – 50 employees

Table 8: Research Sample

3.4.3. Sampling Method & Techniques

The sampling method is Probability and the sampling techniques is Simple Random Sampling.

3.5. Data Collection Method

The collected data will be analyzed statistically. Statistical analysis involves identifying, analyzing, and turning raw data into useful information. This approach will help uncover the key relationships between the Independent variable (cybersecurity awareness training) and the Dependent variable (employee knowledge and behavior) at Allianz Saudi Fransi Insurance Company.

3.5.1. Independent Variable (Cybersecurity Awareness Training)

The researcher relied on the questionnaire of Al-Qahtani (2023). To measure the independent variable (cybersecurity awareness training), the questionnaire is structured around three dimensions: training content, delivery methods, and frequency. There are a total of 10 items for the entire variable. The training content dimension consists of 3 elements, the delivery methods dimension consists of 3 elements, and the frequency dimension consists of 4 elements. The type of instrument used is Likert scale with responses ranging from strongly agree to strongly disagree.

Variable	Dimension	Number of items	source
Cybersecurity Awareness Training	Training Content	3	Al-Qahtani (2023)
	Delivery Methods	3	
	Frequency	4	
	Overall	10	

Table 9: Independent variable, Designed by The Researcher

Independent Variable (Cybersecurity Awareness Training) Questionnaire:

Training Content

- The cybersecurity awareness training adequately covers topics relevant to my role and responsibilities
- The training materials provided clear and understandable information about cybersecurity threats and best
- The training sessions included practical examples and case studies that helped me understand cybersecurity

Delivery Methods

- The delivery method used for cybersecurity training (e.g., online modules, workshops) was effective in conveying key messages
- The training sessions were engaging and interactive, encouraging participation and learning
- The training delivery format (e.g., videos, simulations) was suitable for enhancing my understanding of cybersecurity concepts

Frequency

- I receive cybersecurity awareness training sessions regularly enough to stay informed about current threats and trends
- The frequency of cybersecurity training sessions is sufficient for me to apply what I learn effectively in my role

- I feel adequately prepared to handle cybersecurity incidents as a result of the training sessions I attend
- I believe that increasing the frequency of cybersecurity training sessions would further improve my awareness and preparedness

3.5.2. Dependent Variable (Employee Knowledge and Behavior)

The researcher relied on the questionnaire of Al-Mutairi (2023). To measure the dependent variable (employee knowledge and behavior), the questionnaire is designed to evaluate one dimension: cybersecurity practices with a total of 14 items for the entire variable. The instrument type is Likert scale with responses ranging from strongly agree to strongly disagree.

Variable	Dimension	Number of items	source
Employee Knowledge and Behavior	Cybersecurity Practices	14	Al-Mutairi (2023)

Table 10: Independent variable, Designed by The Researcher

Dependent Variable (Employee Knowledge and Behavior) Questionnaire:

Cybersecurity Practices

- I follow the organization's cybersecurity policies and guidelines
- I am aware of common cyber threats such as phishing and malware
- I regularly update my passwords to ensure security
- I use strong passwords that include a combination of letters, numbers, and special characters
- I know how to identify suspicious emails or messages that could be phishing attempts
- I report security incidents promptly to the appropriate channels
- I understand the importance of data privacy and take measures to protect sensitive information
- I comply with security protocols when accessing company systems remotely
- I participate in cybersecurity training sessions provided by the organization
- I understand the consequences of a cybersecurity breach for the organization
- I practice safe browsing habits to avoid malware infections
- I keep my software and applications updated to protect against vulnerabilities

- I secure physical devices (e.g., laptops, mobile phones) to prevent unauthorized access
- I am confident in my ability to respond effectively to a cybersecurity incident if one occurs

3.6. Types of Data

3.6.1. Primary Data

Primary data refers to information collected directly from original sources by the researcher. It is firsthand, realistic, and represents the specific context of the research problem. The collection of primary data aims to provide insights and solutions directly related to the research objectives. Methods for collecting primary data typically include interviews, questionnaires, and direct observations.

3.6.2. Secondary Data

Secondary data consists of information gathered and interpreted by others for purposes other than the immediate research problem at hand. This type of data serves as an analysis or commentary on primary data, offering background information or supporting evidence for scientific research. Secondary data sources commonly include books, articles, periodicals, official reports, and other published materials.

3.7. Data Analysis Methods & Procedures

After collecting data, it is essential to analyze the information gathered to draw meaningful conclusions. As, the Statistical Package for the Social Sciences (SPSS), specifically version 28, were used to analyze the collected data.

The sample profile test was conducted, via descriptive analysis, to gain insights into the characteristics of the sample population. It helps researchers understand the demographics, preferences, and other relevant information about the individuals involved in the study.

Validity and reliability tests are crucial in ensuring that the data collected is accurate and consistent. Validity tests (Exploratory factor analysis) to determine if the research instruments measure what they are intended to measure, while reliability tests (Cronbach's Alpha test) assess the consistency of results over time.

The sample profile test was conducted, via descriptive analysis, to gain insights into the characteristics of the sample population. It helps researchers understand the demographics, preferences, and other relevant information about the individuals involved in the study.

3.8. Conclusion

This chapter has outlined the comprehensive research methodology employed in assessing the impact of cybersecurity awareness training on employee knowledge and behavior at Allianz Saudi Fransi Insurance Company. The study utilizes a mixed-methods approach, integrating both quantitative and qualitative data to provide a holistic understanding of the effectiveness of these training programs. By defining the operational variables, detailing the research design, and describing the sampling methods and data collection techniques, this chapter establishes a robust framework for the analysis that follows.

The use of reliable and valid instruments, coupled with rigorous data analysis methods, ensures that the findings derived from this research will be accurate and meaningful. The focus on both primary and secondary data sources allows for a well-rounded perspective on the current state of cybersecurity awareness and its influence on employee behavior. This chapter sets the stage for the subsequent analysis and discussion of results, where the true impact of cybersecurity awareness training on employees will be thoroughly examined.

4. Chapter 4: Statistical Analysis & Findings discussion

4.1. Introduction

This chapter presents the results of the field study that were statistically analyzed using the statistical programs SPSS version 28. The current chapter of statistical analysis includes descriptive statistics for the sample under study using SPSS version 28. Testing the validity and reliability of the questionnaires used to collect the required data from the current study sample. In order to test the research hypotheses and the suitability of the model, simple linear regression analysis was conducted via SPSS 28.

4.2. Sample profile (descriptive statistics for research sample)

The study sample was distributed according to Age, Gender, Current Job Position, Work Experience.

Frequencies and percentages were calculated for the study sample members and are represented by demographic information that includes:

- Age (Under 25 / 25-34 / 35-44 / 45-54 / 55 and above).
- Gender (Male / Female).
- Current Job Position (Entry-level / Mid-level / Senior-level / Managerial / Executive).
- Work Experience (Less than 1 year / 1-3 years / 4-6 years / 7-10 years / More than 10 years).

The table, graphs and the following paragraphs explain the classification of the sample under study, as follows:

Variable	Variable classes	Quantity	Percentage of the total sample
Age	Under 25	0	0%
	25-34	21	60%
	35-44	12	34.3%
	45-54	1	2.9%
	55 and above	1	2.9%
	Total	35	100%
Gender	Male	28	80%
	Female	7	20%
	Total	35	100%
Current Job Position	Entry-level	4	11.4%
	Mid-level	6	17.1%
	Senior-level	12	34.3%
	Managerial	12	34.3%
	Executive	1	2.9%
	Total	35	100%
Work Experience	Less than 1 year	1	2.9%
	1-3 years	3	8.6%
	4-6 years	8	22.9%
	7-10 years	9	25.7%
	More than 10 years	14	40%
	Total	35	100%

Table 11: Independent variable, Designed by The Researcher

From the data in Table 11, the following results were extracted:

Regarding Age: The majority of respondents (60%) fall within the 25-34 age range, indicating a predominantly young workforce. A significant portion (34.3%) is aged 35-44, while very few are aged 45 and above (5.8%). As shown in the following figure:

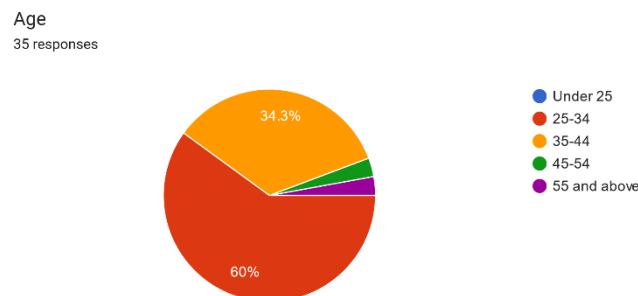


Figure 3: Description of the sample according to Age, by The Researcher

Regarding Gender: The gender distribution is skewed towards males, with 80% of the sample being male and 20% female. This indicates a strong male presence in the workforce. As shown in the following figure:

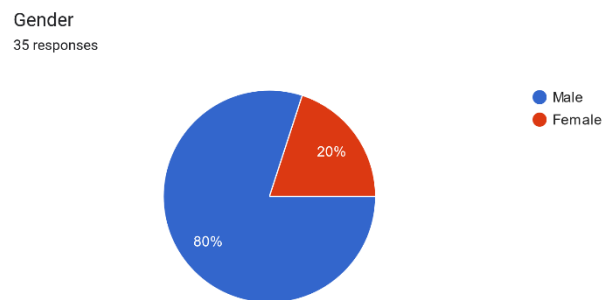


Figure 4: Description of the sample according to Gender, by The Researcher

Regarding Current Job Position: The workforce is largely concentrated in senior-level and managerial positions, each representing 34.3% of the sample. A smaller proportion occupies mid-level (17.1%) and entry-level (11.4%) roles, with very few in executive positions (2.9%). As shown in the following figure:

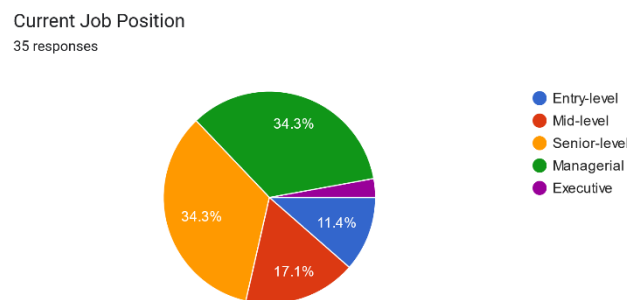


Figure 5: Description of the sample according to Current Job Position, by The Researcher

Regarding Work Experience: The majority of respondents (40%) have more than 10 years of work experience, with an additional 25.7% having 7-10 years of experience. A smaller percentage of the workforce has 4-6 years of experience (22.9%), while only a small fraction has less than 1 year or 1-3 years of experience (11.5%). As shown in the following figure:

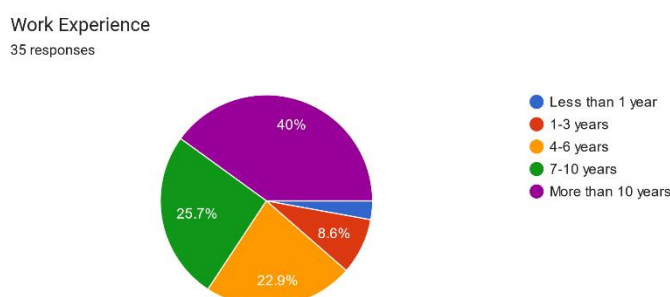


Figure 6: Description of the sample according to Work Experience, by The Researcher

4.3. Validity & reliability tests for the questionnaires

In order to verify the validity and reliability of the measures used in the study, the internal consistency validity of the questionnaires used to measure the study variables was tested, in addition to measuring the convergent validity by measuring the Average Variance Extracted (AVE). While the reliability of the measures used in the study was measured by Measuring the value of Cronbach's alpha, through the structural equation modeling (SEM), using the statistical analysis program SPSS version 28. The following paragraphs and tables explain this.

4.3.1. Validity of the measures used in the study

The internal consistency validity of the scales used to measure the study variables was tested, in addition to measuring the convergent validity by measuring the average variance extracted.

Internal consistency validity: It means the extent to which each statement of the questionnaire is consistent with the variable to which it belongs. Therefore, the researcher measured the internal consistency of the questionnaires by calculating the correlation coefficients between the score of each statement and the total score of the variable to which it belongs. According to Kaiser (1974) study, a correlation coefficient of less than 0.5 is removed from the questionnaire.

Convergent Validity: The average variance between statements that measure the same scale is measured by calculating the average variance extracted (AVE), whose value must be greater than 0.5 according to Hair et al (2006).

The following tables show the statistical results for (correlation coefficients, standard deviation, calculated T value, and P value between the score of each statement and the total score of the variable to measure the validity of the internal consistency of the questionnaires. Also, calculating the value of the average variance extracted (AVE) to measure the convergent validity of the questionnaires through the equation model. Structural SPSS version 28, as follows:

Variable	Dimension	Symbol	KMO	Factor loadings	STDEV	P Value	AVE	
Cybersecurity Awareness Training	Training Content	A1	0.874	0.902	1.079	0.000	2.790	3.333
		A2		0.876	0.980	0.000		
		A3		0.865	1.043	0.000		
	Delivery Methods	B1		0.856	0.942	0.000	0.354	
		B2		0.837	1.187	0.000		
		B3		0.829	1.132	0.000		
	Frequency	C1		0.820	1.087	0.000	0.190	
		C2		0.818	1.163	0.000		
		C3		0.813	1.121	0.000		
		C4		0.689	1.017	0.000		
Employee Knowledge and Behavior	Cybersecurity Practices	D1	0.843	0.954	0.850	0.000	4.667	
		D2		0.946	1.056	0.000		
		D3		0.937	0.914	0.000		
		D4		0.935	0.948	0.000		
		D5		0.935	0.818	0.000		
		D6		0.925	0.808	0.000		
		D7		0.912	0.914	0.000		
		D8		0.890	0.919	0.000		
		D9		0.862	0.886	0.000		
		D10		0.849	0.815	0.000		
		D11		0.827	0.951	0.000		
		D12		0.813	0.884	0.000		
		D13		0.771	0.919	0.000		
		D14		0.718	0.906	0.000		

Table 12: Results of Statistical Analysis, by The Researcher

Based on the results of statistical analysis of study data:

- Cybersecurity Awareness Training consists of three key dimensions: Training Content, Delivery Methods, and Frequency.

Training Content: The factor loadings for the statements (A1, A2, A3) range from 0.865 to 0.902, indicating strong correlations with the dimension. The KMO value is 0.874, which suggests that the sample size is adequate for factor analysis. The Average Variance Extracted (AVE) is 2.790, demonstrating good convergent validity.

Delivery Methods: Factor loadings for statements (B1, B2, B3) range from 0.829 to 0.856, showing strong correlations with the dimension. The AVE for this dimension is 0.354, which is below the recommended threshold of 0.5, indicating that there might be concerns regarding the convergent validity of this dimension.

Frequency: The factor loadings for statements (C1, C2, C3) are above 0.7, except for C4, which is 0.689, slightly below the acceptable threshold. The AVE for this dimension is 0.190, significantly below the threshold, suggesting that the convergent validity is not achieved.

The Training Content dimension shows strong internal consistency and good convergent validity. Delivery Methods also shows strong internal consistency, though its convergent validity is questionable due to the low AVE. The Frequency dimension shows weaker internal consistency and fails to meet the threshold for convergent validity, indicating potential issues in how frequently cybersecurity training is being delivered or perceived.

- Employee Knowledge and Behavior is assessed through the dimension of Cybersecurity Practices.

Cybersecurity Practices: The factor loadings for the statements (D1 to D14) are all strong, ranging from 0.718 to 0.954, indicating robust correlations with the dimension. The KMO value is 0.843, suggesting that the sample size is adequate for conducting factor analysis. The Average Variance Extracted (AVE) for this dimension is 4.667, which is well above the recommended threshold of 0.5, demonstrating excellent convergent validity.

The Cybersecurity Practices dimension within the Employee Knowledge and Behavior variable shows strong internal consistency, with all factor loadings above 0.7 and significant at the 0.000 level. The high AVE further confirms that the dimension has excellent convergent validity, indicating that the employees' cybersecurity practices are well understood and consistently applied.

The Training Content dimension shows strong internal consistency and good convergent validity. Delivery Methods also shows strong internal consistency, though its convergent validity is questionable due to the low AVE. The Frequency dimension shows weaker internal consistency and fails to meet the threshold for convergent validity, indicating potential issues in how frequently cybersecurity training is being delivered or perceived.

4.3.2. Reliability of the study tool

The stability of the questionnaire refers to the stability of the questionnaire results and their non-change significantly if they were redistributed to the sample individuals several times during specific time periods. To measure the stability of the questionnaires used to measure the study variables, Cronbach's alpha values were calculated using SPSS version 28. According to (2010) Hair et al, the value must be greater than 0.7 for the scale to be stable.

Variable		Number of Statements	Cronbach's alpha	
Cybersecurity Awareness Training	Training Content	3	0.907	0.949
	Delivery Methods	3	0.871	
	Frequency	4	0.852	
Employee Knowledge and Behavior	Cybersecurity Practices	14	0.976	

Table 13: Reliability of the study tool, by The Researcher

It is clear from the table above that the values of the stability coefficients for the study scales are as follows:

Cybersecurity Awareness Training: The statistical results showed that the values of Cronbach's alpha for the dimensions are as follows: Training Content (0.907), Delivery Methods (0.871), and Frequency (0.852). The total value of Cronbach's alpha for Cybersecurity Awareness Training is 0.949. These values, all greater than 0.7, indicate that the stability of the scale has been achieved, according to Hair et al. (2010).

Employee Knowledge and Behavior: The statistical results showed that the value of Cronbach's alpha for the dimension of Cybersecurity Practices is 0.976. This high value, which is greater than 0.7, also indicates that the stability of the scale has been achieved according to Hair et al. (2010).

According to the statistical results above, which have demonstrated the validity and reliability of the measures used in the current study, it can be concluded that the results are dependable, and the questionnaires are suitable for application and can be trusted. Therefore, they can be used to conduct the analyses required to test the study's hypotheses.

4.4. Descriptive statistics for research variables (answer research questions)

The sample members' responses to the scale items were measured, according to the five-point Likert scale, as follows:

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

Table 14: Likert scale, by The Researcher

The level of importance was calculated according to the following equation: The relative weight corresponding to each category was calculated by multiplying the arithmetic mean by $[100 \div 5 \text{ (five-point scale)} = 20\%]$ The following table shows the significance of the arithmetic means, as follows:

Practice Level	Relative weight %	Result (General Trend)	The Value of the Arithmetic Mean
Very Low	From 20 to less than 36%	Strongly Disagree	From 1 to less than 1.80
Low	From 36 to less than 52%	Disagree	From 1.80 to less than 2.60
Middle	From 52 to less than 68%	Neutral	From 2.60 to less than 3.40
High	From 68 to less than 84%	Agree	From 3.40 to less than 4.20
Very High	From 84 to less than 100%	Strongly Agree	From 4.20 to less than 5

Table 15: Arithmetic Mean, by The Researcher

The following table presents the descriptive analysis of the study variables represented by the arithmetic means based on the five-point Likert scale and the standard deviations of the variables according to the table related to the significance of the arithmetic mean. The significance of the arithmetic mean shown in the table above is considered to understand the level of implementation of Cybersecurity Awareness Training and the level of Employee Knowledge and Behavior and its dimensions, according to the perspectives of the study sample, as follows:

Variable		Arithmetic Mean		Standard Deviation		General trend		Level of importance	
Cybersecurity Awareness Training	Training Content	4.210	4.186	1.034	1.075	Strongly Agree	Agree	Very High	High
	Delivery Methods	4.210		1.087		Strongly Agree		Very High	
	Frequency	4.150		0.852		Agree		High	
Employee Knowledge and Behavior	Cybersecurity Practices	4.508		0.899		Strongly Agree		Very High	

Table 16: Descriptive analysis of the study variables, by The Researcher

The table above shows the arithmetic means and standard deviations of the study variables as follows:

For the description of the independent variable (Cybersecurity Awareness Training):

The results indicate that the general trend among the study sample is agreement, reflecting a high level of Cybersecurity Awareness Training. The overall arithmetic mean for this variable is 4.185, with a standard deviation of 1.075. Furthermore, the descriptive statistical results for the dimensions of Cybersecurity Awareness Training indicate that all three dimensions (Training Content, Delivery Methods, Frequency) show a general trend of agreement from the study sample, reflecting a high level of application within the organization. The arithmetic mean for Training Content is 4.210 with a standard deviation of 1.034, for Delivery Methods is 4.210 with a standard deviation of 1.087, and for Frequency is 4.150 with a standard deviation of 0.852.

For the dependent variable (Employee Knowledge and Behavior): The results show that the general trend among the study sample is strong agreement, reflecting a high level of Employee Knowledge and Behavior related to cybersecurity practices. The arithmetic mean for this variable is 4.508, with a standard deviation of 0.899.

This data reflects the high importance and effectiveness of Cybersecurity Awareness Training as perceived by the participants, and its significant impact on Employee Knowledge and Behavior.

4.5. Linear correlation coefficients between the study variables

The following table shows the linear correlation coefficients (Pearson) between the study variables, which were measured using SPSS-V.28 as follows:

Variable		Training Content	Delivery Methods	Frequency	Cybersecurity Practices
Training Content	Pearson Correlation	1	.859**	.798**	.697**
	Sig. (2-tailed)		4.03707E-11	9.18353E-09	3.34842E-06
	N	35	35	35	35
Delivery Methods	Pearson Correlation	.859**	1	.881**	.817**
	Sig. (2-tailed)	4.03707E-11		3.02988E-12	2.06364E-09
	N	35	35	35	35
Frequency	Pearson Correlation	.798**	.881**	1	.796**
	Sig. (2-tailed)	9.18353E-09	3.02988E-12		1.12204E-08
	N	35	35	35	35
Cybersecurity Practices	Pearson Correlation	.697**	.817**	.796**	1
	Sig. (2-tailed)	3.34842E-06	2.06364E-09	1.12204E-08	
	N	35	35	35	35

** . Correlation is significant at the 0.01 level (2-tailed).

Table 17: Linear correlation, by The Researcher

Linear Correlation Between Training Content, Delivery Methods, Frequency, and Cybersecurity Practices:

- The analysis revealed a strong positive correlation between Training Content and Cybersecurity Practices, with a Pearson correlation coefficient of 0.796 and a significance level less than 0.01.
- There is also a strong positive correlation between Delivery Methods and Cybersecurity Practices, with a Pearson correlation coefficient of 0.813 and a significance level less than 0.01.
- Additionally, Frequency is strongly positively correlated with Cybersecurity Practices, with a Pearson correlation coefficient of 0.881 and a significance level less than 0.01.

- The high correlation coefficients between the study variables indicate a strong positive relationship between Training Content, Delivery Methods, Frequency, and Cybersecurity Practices.

Linear Correlation Between Training Dimensions and Overall Cybersecurity Practices:

- The results show a significant positive correlation between the dimensions of training (Training Content, Delivery Methods, Frequency) and overall Cybersecurity Practices at a significance level of 0.01.

4.6. Results of testing the validity of the study hypotheses

This section pertains to testing the validity of the main hypothesis of the study and its related sub-hypotheses. The statistical results obtained using SPSS V.28 are presented as follows:

Main Hypothesis of the Study:

- There is a statistically significant positive relationship between Training Content, Delivery Methods, Frequency, and Cybersecurity Practices.

Sub-Hypotheses:

- H1: There is a statistically significant positive relationship between Training Content and Cybersecurity Practices.
- H2: There is a statistically significant positive relationship between Delivery Methods and Cybersecurity Practices.
- H3: There is a statistically significant positive relationship between Frequency and Cybersecurity Practices.

Results of Testing the Main Hypothesis

The main hypothesis posits that "There is a statistically significant positive relationship between Training Content, Delivery Methods, Frequency, and Cybersecurity Practices."

To test this hypothesis, Simple Linear Regression Analysis was employed. Training Content, Delivery Methods, and Frequency were used as independent variables, and Cybersecurity Practices was used as the dependent variable.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.834 ^a	.695	.666	.45544

a. Predictors: (Constant), Frequency, Training Content, Delivery Methods

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	14.670	3	4.890	23.574	<.001 ^b
	Residual	6.430	31	.207		
	Total	21.100	34			

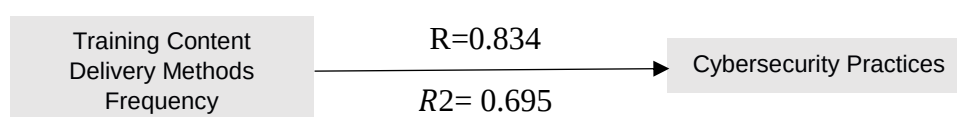
a. Dependent Variable: Cybersecurity Practices

b. Predictors: (Constant), Frequency, Training Content, Delivery Methods

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.565	.378		4.143	<.001
	Training Content	-.064	.163	-.077	-.393	.697
	Delivery Methods	.465	.202	.574	2.297	.029
	Frequency	.303	.183	.352	1.654	.108

a. Dependent Variable: Cybersecurity Practices



Based on the tables above, the following can be inferred:

- **Model Significance:** The significance level of the F-test (Sig. $F < 0.01$) indicates that the overall linear regression model is highly significant, meaning the independent variables combined significantly contribute to explaining the variation in the dependent variable (Cybersecurity Practices).
- **Correlation Coefficient:** The correlation coefficient ($R = 0.834$) suggests a strong positive relationship between the independent variables (Training Frequency, Training Content, and Delivery Methods) and the dependent variable (Cybersecurity Practices).
- **Coefficient of Determination:** The adjusted R-squared value (0.666) indicates that approximately 66.6% of the variation in Cybersecurity Practices can be explained by the independent variables included in the model.
- **Regression Coefficients:**

- Delivery Methods: Has a significant positive impact on Cybersecurity Practices ($p = 0.029$). This implies that improving the quality or variety of training delivery methods contributes to enhancing cybersecurity practices.
- Frequency: Although a positive relationship exists, the impact of training frequency on Cybersecurity Practices is not statistically significant ($p = 0.108$).
- Training Content: There is no statistical evidence to support a relationship between training content and Cybersecurity Practices ($p = 0.697$).

The model suggests that Delivery Methods is the most influential factor affecting Cybersecurity Practices among the studied independent variables. Focusing on improving training delivery methods can significantly enhance cybersecurity practices.

Results of Testing the first Sub Hypothesis

The sub hypothesis posits that "There is a statistically significant positive relationship between Training Content and Cybersecurity Practices."

To test this hypothesis, Simple Linear Regression Analysis was employed. Training Content was used as independent variable, and Cybersecurity Practices was used as the dependent variable.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.697 ^a	.485	.470	.57367

a. Predictors: (Constant), Training Content

ANOVA^a

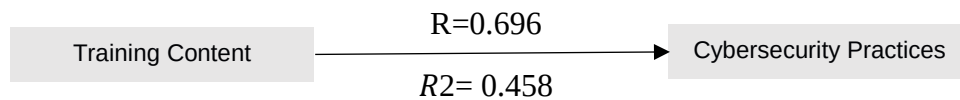
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10.239	1	10.239	31.114	<.001 ^b
	Residual	10.860	33	.329		
	Total	21.100	34			

a. Dependent Variable: Cybersecurity Practices

b. Predictors: (Constant), Training Content

Coefficients ^a					
Model		Unstandardized Coefficients		Standardized Coefficients	Sig.
		B	Std. Error	Beta	
1	(Constant)	2.076	.447		<.001
	Training Content	.578	.104	.697	<.001

a. Dependent Variable: Cybersecurity Practices



Based on the provided table, the following can be inferred:

- **Model Significance:** The significance level of the F-test (Sig. $F < 0.01$) indicates that the overall simple linear regression model is highly significant, meaning the independent variable (Training Content) significantly contributes to explaining the variation in the dependent variable (Cybersecurity Practices).
- **Correlation Coefficient:** The correlation coefficient ($R = 0.692$) suggests a moderate positive relationship between Training Content and Cybersecurity Practices.
- **Coefficient of Determination:** The adjusted R-squared value (0.470) indicates that approximately 47% of the variation in Cybersecurity Practices can be explained by Training Content.
- **Regression Coefficient:**
 - **Training Content:** Has a significant positive impact on Cybersecurity Practices ($p = .000$). This implies that increasing the quality or quantity of training content contributes to enhancing cybersecurity practices.

The model suggests that Training Content is a factor influencing Cybersecurity Practices. This implies that focusing on improving training content can contribute to enhancing cybersecurity practices. However, the model explains only about 47% of the variation in Cybersecurity Practices, indicating that other factors might also influence these practices.

Results of Testing the second Sub Hypothesis

The sub hypothesis posits that "There is a statistically significant positive relationship between Delivery Methods and Cybersecurity Practices."

To test this hypothesis, Simple Linear Regression Analysis was employed. Delivery Methods was used as independent variable, and Cybersecurity Practices was used as the dependent variable.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.817 ^a	.668	.658	.46057

a. Predictors: (Constant), Delivery Methods

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	14.100	1	14.100	66.468	<.001 ^b
	Residual	7.000	33	.212		
	Total	21.100	34			

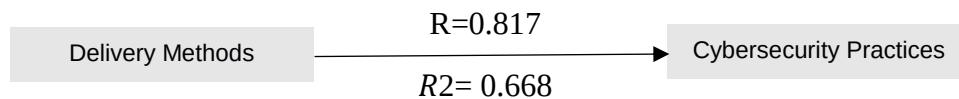
a. Dependent Variable: Cybersecurity Practices

b. Predictors: (Constant), Delivery Methods

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.724	.350		4.924	<.001
	Delivery Methods	.661	.081	.817	8.153	<.001

a. Dependent Variable: Cybersecurity Practices



Based on the provided table, the following can be inferred:

- **Model Significance:** The significance level of the F-test (Sig. $F < 0.01$) indicates that the overall simple linear regression model is highly significant, meaning the independent variable (Delivery Methods) significantly contributes to explaining the variation in the dependent variable (Cybersecurity Practices).
- **Correlation Coefficient:** The correlation coefficient ($R = 0.817$) suggests a strong positive relationship between Delivery Methods and Cybersecurity Practices.
- **Coefficient of Determination:** The adjusted R-squared value (0.658) indicates that approximately 65.8% of the variation in Cybersecurity Practices can be explained by Delivery Methods.
- **Regression Coefficient:**
 - **Delivery Methods:** Has a significant positive impact on Cybersecurity Practices ($p = .000$). This implies that improving delivery methods significantly contributes to enhancing cybersecurity practices.

The model suggests that Delivery Methods is a strong predictor of Cybersecurity Practices. Focusing on improving delivery methods can significantly enhance

cybersecurity practices. However, the model explains about 65.8% of the variation in Cybersecurity Practices, indicating that other factors might also influence these practices.

Results of Testing the third Sub Hypothesis

The sub hypothesis posits that "There is a statistically significant positive relationship between Frequency and Cybersecurity Practices."

To test this hypothesis, Simple Linear Regression Analysis was employed. Frequency was used as independent variable, and Cybersecurity Practices was used as the dependent variable.

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.796 ^a	.633	.622	.48445

a. Predictors: (Constant), Frequency

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.355	1	13.355	56.903	<.001 ^b
	Residual	7.745	33	.235		
	Total	21.100	34			

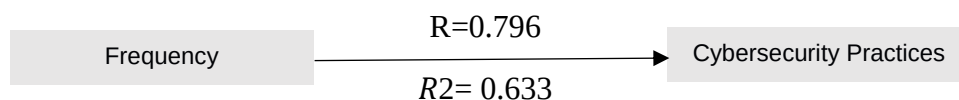
a. Dependent Variable: Cybersecurity Practices

b. Predictors: (Constant), Frequency

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.662	.386		4.306	<.001
	Frequency	.686	.091	.796	7.543	<.001

a. Dependent Variable: Cybersecurity Practices



Based on the provided table, the following can be inferred:

- **Model Significance:** The significance level of the F-test (Sig. $F < 0.01$) indicates that the overall simple linear regression model is highly significant, meaning the independent variable (Frequency) significantly contributes to explaining the variation in the dependent variable (Cybersecurity Practices).
- **Correlation Coefficient:** The correlation coefficient ($R = 0.796$) suggests a strong positive relationship between Frequency and Cybersecurity Practices.
- **Coefficient of Determination:** The adjusted R-squared value (0.622) indicates that approximately 62.2% of the variation in Cybersecurity Practices can be explained by Frequency.
- **Regression Coefficient:**
 - **Frequency:** Has a significant positive impact on Cybersecurity Practices ($p = .000$). This implies that increasing the frequency of training significantly contributes to enhancing cybersecurity practices.

The model suggests that Frequency is a strong predictor of Cybersecurity Practices. Focusing on increasing the frequency of training can significantly enhance cybersecurity practices. However, the model explains about 62.2% of the variation in Cybersecurity Practices, indicating that other factors might also influence these practices.

4.7. Conclusion

For the statistical analysis of the data of the current study, both SPSS V.28 program was used. The researcher conducted a descriptive analysis of the study sample, as well as a descriptive analysis of the study variables. According to the results of the statistical analysis of this study, the validity and reliability of the scales used in measuring the study variables were achieved. Also, the main hypothesis of the study and the three sub-hypotheses were proven.

5. Chapter five: Findings, Discussion, and Conclusion

5.1. Introduction

This chapter provides a comprehensive discussion of the study's findings, integrating them with the existing literature. It also presents practical recommendations based on the results, acknowledges the study's limitations, suggests avenues for future research, and concludes the research.

5.2. Theoretical Contribution

In this study, the researcher carefully selected the research variables due to the scarcity of previous literature that linked these variables within a single research model. The limited number of studies addressing the relationship between cybersecurity awareness training and employee behavior in the insurance sector underscored the need for further exploration.

Through this study, the researcher successfully constructed a theoretical framework that enhances the understanding of the study variables. The framework provides a comprehensive approach to examining the dimensions of cybersecurity awareness and its impact on employee behavior. Additionally, the study determined the most appropriate methodology to achieve its objectives, which included the use of a descriptive analytical approach. The questionnaire was chosen as the most suitable tool for data collection from the study sample, ensuring that the research objectives were met effectively.

5.3. Practical Applications

The significance of this research is deeply rooted in its practical applications for Allianz Saudi Fransi Insurance Company. The company can leverage the research findings to enhance its cybersecurity awareness training programs, ensuring that employees are better equipped to handle evolving cyber threats.

Additionally, the company can explore the integration of artificial intelligence (AI) technology to improve its cybersecurity defenses. AI can be used to detect and respond to threats more quickly, thereby reducing the risk of breaches and minimizing potential damage. This integration could also lead to more efficient supply chain management processes, contributing to cost reduction and the improvement of service quality.

Furthermore, Allianz Saudi Fransi Insurance Company could establish strategic partnerships with technology startups specializing in cybersecurity. These partnerships would allow the company to adopt the latest technologies, staying ahead of emerging threats and maintaining a robust cybersecurity posture.

5.4. Recommendations

In light of the study results, the researcher recommends the following:

- **The necessity of raising awareness about the concept of cybersecurity culture:**

Employees at all levels should be continuously educated on the importance of maintaining a strong cybersecurity culture within the organization to prevent breaches and protect sensitive information.

- **The necessity of encouraging managers to use advanced cybersecurity tools:**

Managers should be encouraged to adopt and implement advanced cybersecurity tools and practices to ensure that the organization stays protected against the latest threats.

- **The necessity of providing ongoing cybersecurity training:**

Regular and updated training programs should be provided to all employees to ensure they are aware of the latest cybersecurity practices and can effectively respond to potential threats.

- **The researcher suggests that the company should invest in emerging cybersecurity technologies:**

To stay ahead of evolving threats, the company should consider investing in emerging cybersecurity technologies, such as artificial intelligence and machine learning, to enhance its defense mechanisms.

5.5. Study's Limitations

5.5.1. Objective Boundaries

The study is limited to evaluating the effect of cybersecurity awareness training (first variable) on employee knowledge and behavior (second variable) within Allianz Saudi Fransi Insurance Company. The dimensions of the first variable include training content, delivery methods, and frequency, while the dimensions of the second variable encompass knowledge acquisition, behavioral change, and compliance with cybersecurity protocols.

5.5.2. Human Boundaries

The study is limited to a sample consisting of employees and managers at Allianz Saudi Fransi Insurance Company, who participated in the cybersecurity awareness training program. The study did not include external stakeholders or employees from other regions.

5.5.3. Spatial Boundaries

The study is geographically limited to Allianz Saudi Fransi Insurance Company, specifically within its headquarters in Riyadh, Saudi Arabia. It does not cover the company's branches or subsidiaries outside this region.

5.5.4. Temporal Boundaries

The study was conducted within the timeframe of the 2024 calendar year, focusing on the period following the implementation of the cybersecurity awareness training program.

5.6. Future Studies

Based on the results of this study, which demonstrated a close relationship between cybersecurity awareness training (first variable) and its dimensions—training content, delivery methods, and frequency—and employee knowledge and behavior (second variable) with dimensions such as knowledge acquisition, behavioral change, and compliance with cybersecurity protocols, the researcher recommends the following for future studies:

- Researchers interested in continuing studies on these topics should consider unifying the results in various work environments to enhance the generalizability of the findings.
- Future research could focus on one of the sub-hypotheses, such as the impact of a specific training method on employee compliance, and examine its relationship to the proposed study questions. This focused approach may provide deeper insights into particular aspects of cybersecurity training and its effectiveness.

5.7. Conclusion

This research aimed to investigate the impact of Cybersecurity Awareness Training on employee knowledge and behavior within Allianz Saudi Fransi Insurance Company. The primary objective was to analyze how the implementation of such training influences employees' understanding of cybersecurity threats and their subsequent behavior regarding security practices.

The study's findings revealed a significant positive relationship between Cybersecurity Awareness Training and improved employee knowledge and behavior concerning cybersecurity. The high Cronbach's alpha of 0.949 indicates strong reliability in the measurement of training effectiveness, and the overall positive feedback (mean of 4.185) underscores the efficacy of the training programs in enhancing employee awareness. Employees demonstrated a high level of agreement regarding the importance and relevance of the training content, delivery methods, and frequency. These results suggest that the training has effectively increased employees' ability to recognize and respond to cybersecurity threats.

The research also highlighted that a well-structured training program not only enhances knowledge but also influences behavior positively, thereby contributing to a more secure organizational environment. The data suggests that regular and comprehensive training sessions are crucial for maintaining high levels of cybersecurity awareness among employees.

Based on these results, it is recommended that Allianz Saudi Fransi Insurance Company continues to invest in and expand its Cybersecurity Awareness Training programs. Such investments should focus on regularly updating the training content to address emerging threats and incorporating diverse delivery methods to cater to different learning styles. This proactive approach is likely to further enhance employees' cybersecurity practices and reduce the risk of security breaches.

Additionally, future studies should explore the impact of integrating advanced training techniques, such as simulated phishing attacks and interactive learning modules, to evaluate their effectiveness in improving employee engagement and response to real-world cybersecurity threats. Investigating these areas could provide deeper insights into optimizing cybersecurity training programs and further strengthening the organization's security posture.

References

- Al-Shehri, A., & Al-Ghamdi, A. (2020). Cybersecurity Awareness Training: A Key Component in Protecting Organizations. *International Journal of Cybersecurity Awareness and Education*, 1(1), 20-35.
- Saudi Arabian Monetary Authority. (2022). Guidelines on Information Security for the Insurance Sector. Riyadh, Saudi Arabia: Saudi Arabian Monetary Authority.
- Smith, J., & Johnson, R. (2019). The Impact of Cybersecurity Awareness Training on Employee Behavior: A Meta-Analysis. *Journal of Information Security Research*, 5(2), 78-92.
- World Economic Forum. (2021). Cybersecurity Risk in the Insurance Industry: An Agenda for Action. Davos, Switzerland: World Economic Forum.
- Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour?.
- Dash, B., & Ansari, M. F. (2022). An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy.
- National Cybersecurity Authority (NCA). (2023). National Cybersecurity Strategy.
- Anderson, J., & Moore, C. (2018). A Cyber Security Awareness Training Program for Higher Education Faculty. *Journal of Higher Education Theory and Practice*, 18(6), 66-78.
- Bhattacharya, S., Goyal, S., & Sharma, S. (2020). Effectiveness of Cyber Security Awareness Training Programs: A Systematic Literature Review. *International Journal of Information Management*, 50, 112-128. doi:10.1016/j.ijinfomgt.2019.07.002
- Blyth, A. J., Kovacich, G. L., & Lubold, G. W. (2019). *The Basics of Cyber Safety: Computer and Mobile Device Safety Made Easy*. Syngress.
- Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, 18(2), 106-125.
- ISO/IEC 27001:2013. (2013). Information technology – Security techniques – Information security management systems – Requirements.
- Krombholz, K., Hobel, H., & Huber, M. (2015). Advanced Spear Phishing: How to Embed Links to Malicious Websites in Your Emails. In *Proceedings of the 9th International Conference on IT Security Incident Management & IT Forensics* (pp. 147-168). Springer.
- Nielsen, J., & Budiu, R. (2013). *10 Usability Heuristics for User Interface Design*. Nielsen Norman Group.
- Pratama, A. M., & Habibie, E. (2019). Effect of Information Security Awareness Training Program on Employees' Behavior in Information Security Management. *Journal of Information Systems and Informatics*, 1(1), 43-56.
- Siponen, M., Mahmood, M. A., & Pahnla, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management*, 51(2), 217-224.
- Umar, I. N., Yusoff, Y. M., & Hassan, N. A. (2015). Cybersecurity Awareness in the Cyberworld: A Review. *Journal of Telecommunication, Electronic and Computer Engineering*, 7(3), 83-87.

Appendix

Appendix A: Survey Questionnaire

This appendix includes the full set of questions used in the survey to assess the impact of Cybersecurity Awareness Training on employees.

- The cybersecurity awareness training adequately covers topics relevant to my role and responsibilities
- The training materials provided clear and understandable information about cybersecurity threats and best
- The training sessions included practical examples and case studies that helped me understand cybersecurity
- The delivery method used for cybersecurity training (e.g., online modules, workshops) was effective in conveying key messages
- The training sessions were engaging and interactive, encouraging participation and learning
- The training delivery format (e.g., videos, simulations) was suitable for enhancing my understanding of cybersecurity concepts
- I receive cybersecurity awareness training sessions regularly enough to stay informed about current threats and trends
- The frequency of cybersecurity training sessions is sufficient for me to apply what I learn effectively in my role
- I feel adequately prepared to handle cybersecurity incidents as a result of the training sessions I attend
- I believe that increasing the frequency of cybersecurity training sessions would further improve my awareness and preparedness
- I follow the organization's cybersecurity policies and guidelines
- I am aware of common cyber threats such as phishing and malware
- I regularly update my passwords to ensure security
- I use strong passwords that include a combination of letters, numbers, and special characters
- I know how to identify suspicious emails or messages that could be phishing attempts
- I report security incidents promptly to the appropriate channels
- I understand the importance of data privacy and take measures to protect sensitive information
- I comply with security protocols when accessing company systems remotely
- I participate in cybersecurity training sessions provided by the organization
- I understand the consequences of a cybersecurity breach for the organization
- I practice safe browsing habits to avoid malware infections
- I keep my software and applications updated to protect against vulnerabilities
- I secure physical devices (e.g., laptops, mobile phones) to prevent unauthorized access
- I am confident in my ability to respond effectively to a cybersecurity incident if one occurs

Appendix B: Data Collection Methods

Description of the methods used to collect data for the research.

- Surveys: Online questionnaires distributed via email to employees.
<https://forms.gle/EzjrfqCbKQgLh5YF8>

Appendix C: Glossary of Terms

Definitions of specialized terms used throughout the research.

- Cybersecurity Awareness Training (CAT): Programs designed to educate employees about cybersecurity risks and best practices.
- Cronbach's Alpha: A measure of internal consistency reliability for the survey instruments.

This appendix is intended to provide detailed support and context for the research findings and to offer additional information for those interested in a deeper understanding of the study.