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

Dedication

Abstract

Purpose:

Methodology:

Findings:

Originality & Implication:

Keywords:

Table of Contents

Acknowledgment 1

Dedication 2

Abstract 3

1. Chapter 1: Introduction 8

1.1. Research Background 9

1.2. Research Problem 10

1.2.1. Theoretical Gaps 10

1.2.2. Practical Gaps 10

1.3. Research Significance 11

1.3.1. At the theoretical level 11

1.3.2. At the practical level 11

1.4. Research Questions 12

1.5. Research Objectives 12

1.5.1. General Objective 12

1.5.2. Sub-Objectives 13

1.6. Research Hypotheses 13

1.6.1. Main Hypothesis (H1) 13

1.6.2. Sub- Hypotheses 14

1.7. Research Model 14

1.7.1. Dimensions of the Independent Variable 15

1.7.2. Dimensions of the Dependent Variable 15

1.7.3. Research Model Diagram 16

1.8. Scope of The Study 17

1.9. The Project Structure 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 36
2.5. Conclusion 37
3. Chapter 3: Research Methodology 39
3.1. Introduction 40
3.2. Operational definitions for research variables 40
3.2.1. Cybersecurity Awareness Training 40
3.2.2. Employee Knowledge 41
3.2.3. Employee Behavior 41
3.2.4. Perceived Benefits and Challenges of Training 41
3.2.5. Effectiveness of Cybersecurity Awareness Training 42
3.3. Research design (research onion) 42
3.4. Research population & Sampling methods and technique 43
3.4.1. Research Population 43
3.4.2. Research Sample 43
3.4.3. Sampling Method & Techniques 43
3.5. Data Collection Method 44

3.5.1. Independent Variable (Cybersecurity Awareness Training) 44
3.5.2. Independent Variable (Cybersecurity Awareness Training) 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 48
4.4. Descriptive statistics for research variables (answer research questions) 49
4.5. Testing Hypotheses & Findings Discussion 49
4.6. Conclusion 49
5. Chapter five: Research limitations, Recommendations & Conclusion 50
5.1. Research Limitations & Future Research 51
5.2. Research Recommendations 51
References 52
Appendix 52

List of Figures:

Figure Number	Figure Title	Page Number
Figure 1	Research Model Diagram (The Researcher, 2024)	16
Figure 2	Research Design (The Researcher, 2024)	42

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)	36
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)	43
Table 8	Research Sample (Research population & Sampling methods and technique, 3.4.2)	43
Table 9	Independent variable (Data Collection Method, 3.5.1)	44
Table 10	Dependent variable (Data Collection Method, 3.5.2)	44

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

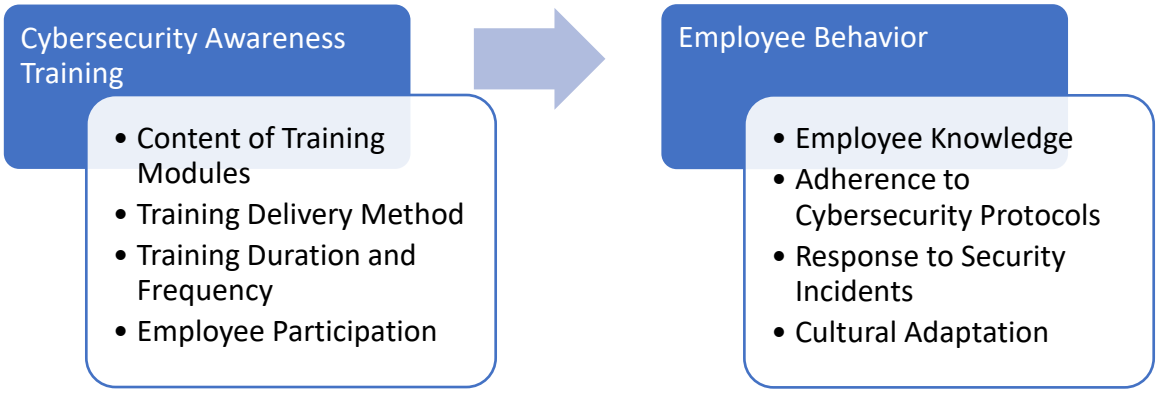

Figure 1: Designed by The Researcher

1.8. Scope of The Study

1.9. The Project Structure

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 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: nother 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)

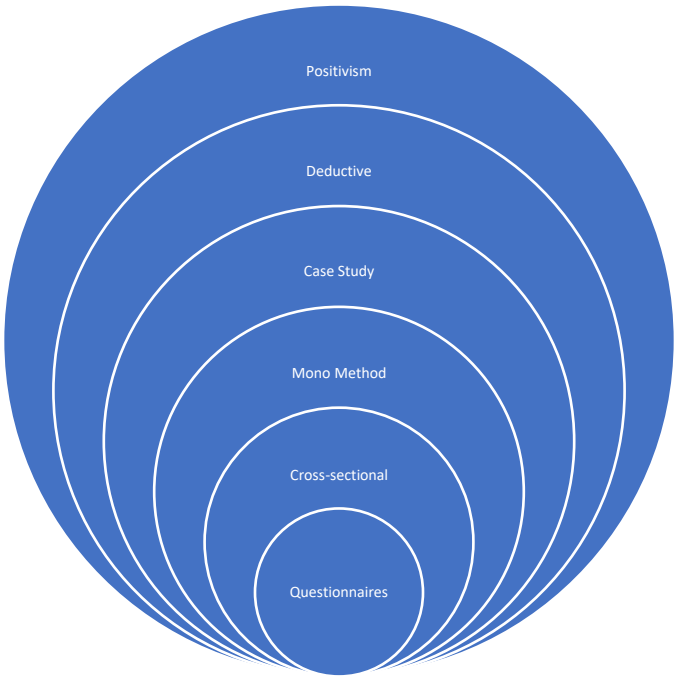

Figure 2: Designed by The Researcher

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

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 9: Independent variable, Designed by The Researcher

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` 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

4. Chapter 4: Statistical Analysis & Findings discussion

4.1. Introduction

4.2. Sample profile (descriptive statistics for research sample)

4.3. Validity & reliability tests for the questionnaires

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

4.5. Testing Hypotheses & Findings Discussion

4.6. Conclusion

5. Chapter five: Research limitations, Recommendations & Conclusion

5.1. Research Limitations & Future Research

5.2. Research Recommendations

5.3. Conclusion

References

Appendix

The Effect of Cybersecurity Awareness Training on Employee Knowledge and Behavior Questionnaire

https://forms.gle/EzjrfqCbKQgLh5YF8