

Midocean University

Faculty of Management

Bachelor of Project Management



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

A Case Study of Allianz Saudi Fransi Insurance Company in
Riyadh, Saudi Arabia

Abubaker Hussain Alattas

2021202957

Final Project 1

Faculty of Management - Midocean University

Supervisor

Dr. Mona Moustafa Elashry

Faculty Member - Faculty of Management - Midocean University

1st Trimester 2024

Table of Contents

Contents

Table of Contents	2
Introduction	3
Research Problem	4
Theoretical gaps:	4
Empirical gaps:	4
Research Significant	5
Theoretical Significance:	5
Empirical Significance:.....	5
Research Questions	6
Research Objectives	6
General Objective:	6
Sub-Objectives:.....	6
Research Hypotheses	7
Main Hypothesis (H1):	7
Sub-Hypotheses:	7
Research Model	8
Dimensions of the Independent Variable:.....	8
Dimensions of the Dependent Variable:	8
Research Model Diagram:	8
Research Methodology	9
References List	10

Introduction

The security landscape in the insurance sector is constantly evolving. While technology adoption fuels efficiency and growth, it also exposes companies to increasingly sophisticated cyber threats. As a key player in the Saudi Arabian market, Allianz Saudi Fransi Insurance recognizes the crucial role of employee awareness in mitigating these risks. The company actively implements cybersecurity training programs, but questions remain about their effectiveness in translating knowledge into secure behavior.

Previous research has explored the impact of such training in diverse organizational settings. Some studies, like "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy" (2022), observe positive impacts on employee knowledge and self-reported behavior changes. However, others, like "The Gap Between Knowledge and Action: Why Cybersecurity Training Often Fails" (2022), highlight the disconnect between acquired knowledge and actual implementation in daily practices.

While these studies provide valuable insights, they often lack context specific to the Saudi Arabian insurance sector and the unique challenges it faces. Additionally, existing research primarily focuses on large-scale surveys and may not capture the nuanced dynamics within individual companies.

This research project aims to address these gaps by conducting a focused case study at Allianz Saudi Fransi Insurance Company in Riyadh. Specifically, it will examine the effect of the company's current cybersecurity awareness training program on employee knowledge and behavior related to threat identification, password hygiene, phishing awareness, and incident reporting.

By delving deeper into the specific context and implementation of training within Allianz Saudi Fransi, this study seeks to:

- Measure the actual impact of the training program on employee knowledge and behavior changes.
- Identify potential knowledge-behavior gaps and analyze their root causes.
- Provide actionable insights for tailoring and improving the training program's effectiveness.

The findings will not only benefit Allianz Saudi Fransi by enhancing their cybersecurity posture, but also contribute valuable knowledge to the broader Saudi Arabian insurance sector and inform policymakers in developing effective training and awareness initiatives. This research ultimately aims to contribute to a more secure and resilient financial landscape in the Kingdom.

Research Problem

As the insurance sector in Saudi Arabia undergoes rapid digital transformation, Allianz Saudi Fransi Insurance Company recognizes the crucial role of employee awareness in mitigating evolving cyber threats. The company actively implements cybersecurity training programs, but questions remain about their effectiveness in translating knowledge into secure behavior.

Theoretical gaps:

Previous studies exploring the impact of cybersecurity awareness training on employee behavior offer valuable insights, but often lack specific context to the Saudi Arabian insurance sector and its unique challenges. Additionally, existing research primarily relies on large-scale surveys, potentially overlooking the nuanced dynamics within individual companies and the effectiveness of training tailored to their specific needs.

Empirical gaps:

While studies have examined the impact of cybersecurity awareness training on employee knowledge and behavior in diverse contexts, there is a scarcity of research focusing on the Saudi Arabian insurance sector. This gap leaves unanswered questions about the effectiveness of such training programs within this specific industry and cultural context. Examining the effect in this setting is crucial to understand how cybersecurity awareness translates to behavior change among insurance professionals in Saudi Arabia.

“To what extent does the current cybersecurity awareness training program at Allianz Saudi Fransi Insurance Company in Riyadh impact employee knowledge and behavior related to threat identification, password hygiene, phishing awareness, and incident reporting?”

By addressing these theoretical and empirical gaps, this research aims to provide a deeper understanding of the effectiveness of cybersecurity awareness training in the Saudi insurance sector and offer valuable insights for improving such programs at Allianz Saudi Fransi and beyond.

Research Significant

While Allianz Saudi Fransi and other insurance companies implement cybersecurity training, questions remain about their effectiveness in translating knowledge into secure behavior. This research aims to address this gap by examining the company's specific training program and its impact on employee behavior.

Theoretical Significance:

This research contributes to the body of knowledge on cybersecurity awareness training in several ways:

- **Contextualizes existing research:** It expands existing research by focusing on the **Saudi Arabian insurance sector**, a unique context with specific challenges and cultural nuances. This adds valuable insights to understanding the effectiveness of training programs in diverse settings.
- **Identifies knowledge-behavior gaps:** By examining the specific training program and employee behavior, the research sheds light on potential gaps between acquired knowledge and actual implementation. This can inform the development of more effective training models that address these specific gaps.
- **Suggests new frameworks:** The findings may contribute to the development and refinement of existing theoretical frameworks for measuring and evaluating the impact of cybersecurity awareness training. This can benefit researchers and practitioners in designing and assessing such programs more effectively.

Empirical Significance:

This research holds significant value for various stakeholders:

- **Allianz Saudi Fransi:** By identifying the impact of their current training program, the research provides actionable insights for improvement, ultimately enhancing their overall cybersecurity posture.
- **Saudi Arabian insurance sector:** Findings can inform other insurance companies in developing and implementing effective training programs, contributing to a more secure sector overall.
- **Policymakers and regulators:** Research findings can highlight gaps in existing regulations and inform future policy development to strengthen cybersecurity awareness within the Saudi Arabian insurance industry.
- **Academic community:** This case study adds valuable data and insights to the existing knowledge on cybersecurity awareness training and its effectiveness in different industry contexts.

By addressing these theoretical and empirical gaps, this research can contribute to a more secure and resilient financial landscape in Saudi Arabia and beyond. It provides valuable insights for practitioners and policymakers in developing and implementing effective cybersecurity training programs, ultimately protecting sensitive information and mitigating cyber threats.

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?

Research Objectives

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.

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.

Research Hypotheses

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.

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.

Research Model

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

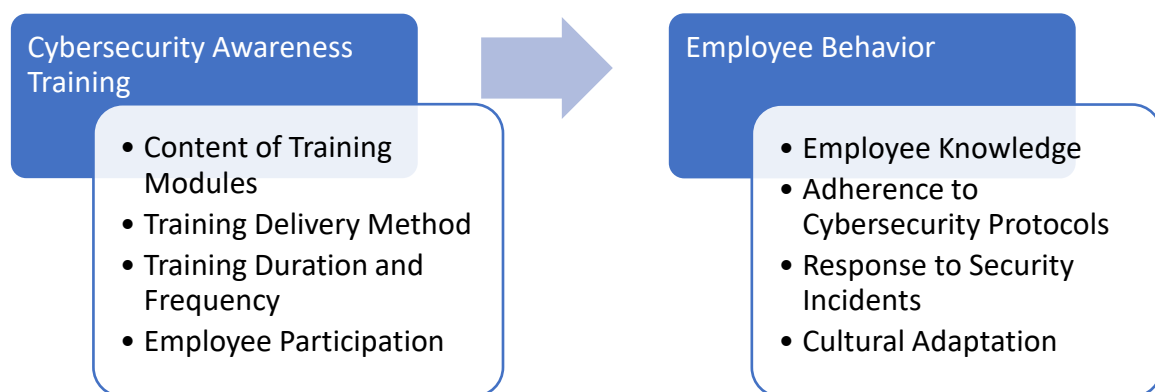
Dimensions of the Independent Variable:

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.

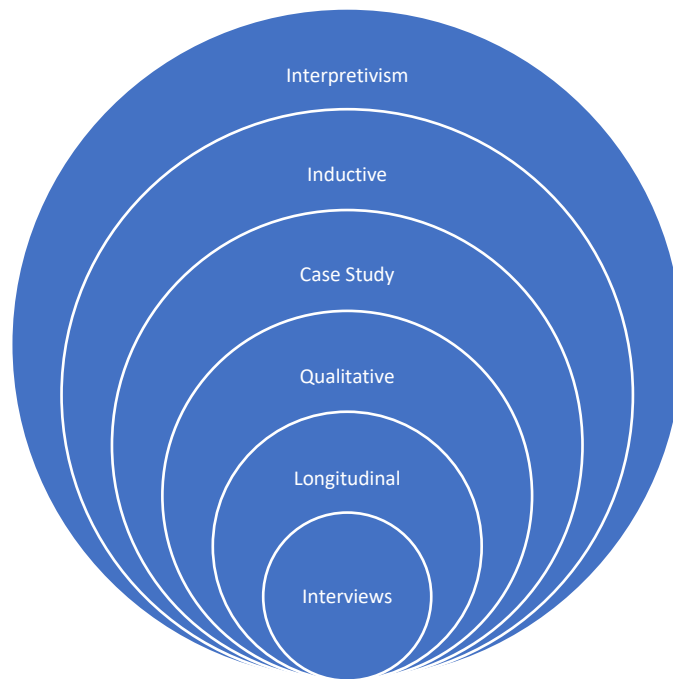
Dimensions of the Dependent Variable:

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.

Research Model Diagram:



Research Methodology



References List

- 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.**