Issue 74, December 2024
DOI: 10.70000/cj.2024.74.616

Cybrarians Journal
E-ISSN 1687-2215

The role of knowledge management in confronting social engineering in the Saudi banking sector: a proposed model

Research – English Summary

Prof. Abdulrashid A. Hafez
Department of Information Science,
King Abdulaziz University, Jeddah, Saudi Arabia
aahafez@kau.edu.sa

Dr. Alhababi Mubarak Alqahtani
Director of Academic Research Department,
King Abdullah College of Command and Staff, Riyadh, Saudi Arabia
hubabi@hotmail.com

Abstract

The great developments in the field of knowledge management, information technology and the resulting acceleration of innovation and increasing the rates of use of smart devices and computerized applications have appeared in return the means and methods of data penetration ,or what is known as social engineering, which has become a real threat to business organizations of all kinds and activities. Hence, it was necessary to have effective systems to protect against penetration and unauthorized use, and since this is one of the basic roles that must be played by knowledge management, the current study seeks to identify the views of officials and workers in the banking sector and the Central Bank in Saudi Arabia to diagnose problems and identify gaps, and then come up with a proposed model based on an integrated set of inputs, treatment and outputs and helps to prevent threats Social Engineering. A focus group consisting of experts and specialists was used to take their observations to come up with the final form of model to be implemented in the banking sector.

Keywords

Knowledge Management, Social Engineering, Financial Fraud, Banking Sector

Introduction

Today's business environment is highly dynamic, fast-paced, and driven by advanced technologies, yet it remains vulnerable to various security threats. Organizational assets, such as digital operations, information, and IT systems, face increasing risks from both internal and external sources, including theft, fraud, sabotage, embezzlement, and espionage. The human element is often considered the weakest link in cybersecurity, as vulnerabilities such as deception, persuasion, and manipulation are frequently exploited.

In this context, knowledge management plays a crucial role in analyzing and understanding how technical and social gaps are leveraged by cybercriminals, enabling the development of effective prevention and protection strategies. Strengthening organizations' ability to combat fraudulent tactics—whether through weaknesses in technical controls or a lack of customer awareness—requires a comprehensive approach. This approach should integrate information technology, organizational culture, and knowledge management processes to formulate effective solutions that mitigate these threats.

The role of knowledge management in countering social engineering involves developing an integrated system that combines technology, organizational culture, and human awareness. This includes fostering a strong information security culture that enhances awareness of social engineering tactics and empowers organizations to detect and resist cybercriminals, even by using their own methods when necessary.

This study aims to develop a comprehensive and effective model that enhances existing prevention frameworks by conducting analytical studies on employee behavior, assessing compliance with security policies, implementing awareness campaigns on social engineering threats, and applying both national and international IT security standards to ensure robust protection.

Study Problem

The rapid advancement of technology has led to a significant transformation in the world, facilitating global connectivity and communication. However, this progress has also given rise to various forms of cybercrime that violate social norms, legal standards, and information security protocols, posing threats to individuals, societies, and organizations. Within this framework, the role of knowledge management in combating social engineering—particularly in the

DOI: 10.70000/cj.2024.74.616

banking sector—becomes increasingly vital. Implementing comprehensive measures and integrated policies is essential to safeguarding security, privacy, and data integrity.

A review of the existing literature indicates that there is a scarcity of studies in the Arab world addressing this issue. Thus, the study seeks to answer the following key question:

What is the role of knowledge management in countering social engineering in the Saudi banking sector?

Significance of the Problem

Despite the efforts made by the Saudi Central Bank and other public and private entities—such as regulatory frameworks, guidelines, and national awareness campaigns—there remains an urgent need for targeted and specialized knowledge management initiatives. These initiatives should include nationwide awareness campaigns, fraud alert messages, and the application of knowledge management principles to better understand and counteract social engineering threats within the banking sector.

Despite ongoing efforts, financial and banking fraud cases continue to emerge in new and sophisticated forms, highlighting the necessity of systematically collecting, analyzing, and distributing critical information to enhance security measures across the Saudi banking industry.

Significance of the Study

The importance of this study stems from the critical nature of social engineering threats and the need for proactive prevention measures. It is also one of the few studies that link knowledge management with social engineering in the banking sector. By exploring the application of knowledge management in Saudi banks, this research contributes to strengthening cybersecurity and fraud prevention strategies.

Additionally, the study addresses a research gap, as few Arab studies have examined financial fraud and its implications in the Saudi banking sector. It is hoped that the findings will assist Saudi banks in adopting an effective knowledge management model to combat social engineering threats.

DOI: 10.70000/cj.2024.74.616

Study Objectives

The primary objective of this study is to propose an integrated knowledge management model to counter social engineering threats in the Saudi banking sector. To achieve this goal, the study aims to:

1. Assess the current state of knowledge management practices in the Saudi banking sector.
2. Evaluate awareness levels regarding prominent social engineering threats in Saudi banks.
3. Identify the roles of knowledge management in combating social engineering.
4. Examine the challenges hindering knowledge management's effectiveness in addressing social engineering threats.
5. Develop a proposed model for leveraging knowledge management to mitigate social engineering risks in the Saudi banking sector.

Study Questions

This study seeks to answer the following primary question:

What is the role of knowledge management in confronting social engineering in the Saudi banking sector, and what is the proposed model to enhance this role?

To address this overarching question, the study explores the following sub-questions:

1. How is knowledge management currently applied in the Saudi banking sector?
2. What is the level of awareness regarding the most significant social engineering threats in the Saudi banking sector?
3. What role does knowledge management play in countering social engineering in the Saudi banking sector?
4. What challenges hinder the effective use of knowledge management in mitigating social engineering threats?
5. What strategies can be proposed to enhance the role of knowledge management in combating social engineering in the Saudi banking sector?

DOI: 10.70000/cj.2024.74.616

Study Scope

This study is focused on the Saudi banking sector, specifically within the jurisdiction of the Saudi Central Bank and financial institutions operating in the central region, particularly Riyadh. The research targets officials from both the Saudi Central Bank and the banking sector in the central region who are directly involved in cybersecurity and fraud prevention.

Study Methodology

The study employs a case study approach alongside a descriptive survey methodology to examine the role of knowledge management in addressing social engineering threats in the Saudi banking sector.

Data Collection Methods:

1. Questionnaire: A structured questionnaire was designed and distributed to a purposive sample of officials from the Saudi Central Bank and the banking sector in the central region who are directly involved in cybersecurity. This aims to assess their awareness and utilization of knowledge management in preventing and mitigating social engineering threats.
2. Focus Group: A focus group discussion was conducted to evaluate the proposed knowledge management model developed in this study. This model was formulated based on an extensive review of literature and studies related to knowledge management and social engineering threats in the banking sector.

By integrating both quantitative and qualitative research methods, this study provides a comprehensive analysis of how knowledge management can be leveraged to strengthen cybersecurity and prevent social engineering attacks in the Saudi banking sector.

Study Results

Based on the analysis of the study data presented in Chapter Four, several key findings were identified in response to the study questions:

- Knowledge Management in the Saudi Banking Sector: The results indicate a high level of recognition of the importance of knowledge management in the Saudi banking sector. This recognition is particularly evident in areas such as enhancing security and protection

DOI: 10.70000/cj.2024.74.616

systems, attracting experts to drive excellence, and implementing precise control strategies. These findings emphasize the crucial role that knowledge management plays in improving security and operational efficiency within the banking industry.

- There was broad agreement among study participants regarding the implementation of knowledge management in the sector. The mean scores of agreement on this aspect ranged between 3.62 and 4.12 on a five-point Likert scale, placing them within the "agree" category. This indicates a consistent perception among officials of the Saudi Central Bank and banking sector professionals in the central region regarding the application of knowledge management.
- Awareness of Social Engineering and Cybersecurity Threats: The findings highlight a strong consensus on the significance of raising awareness about social engineering threats and cybersecurity risks in the banking sector. Notably, concerns were raised about the risks of sharing personal data online and the importance of using verified software and trusted websites for downloads.
- The results also revealed some variation in awareness levels among participants. The mean scores of agreement on awareness of social engineering threats ranged from 3.73 to 4.35, indicating that while awareness is generally high, there are differences in individual perceptions. These findings suggest that awareness campaigns should be further tailored to address gaps in understanding.
- Role of Knowledge Management in Countering Social Engineering: The study participants demonstrated general agreement on the role of knowledge management in combating social engineering threats. Responses were consistent, with mean agreement scores ranging from 3.58 to 4.17, reflecting a strong belief in the effectiveness of knowledge management strategies.
- The findings highlight several key functions of knowledge management, including:
    - Safeguarding sensitive information and IT assets
    - Leveraging artificial intelligence and advanced software solutions to counter social engineering tactics

DOI: 10.70000/cj.2024.74.616

- Enhancing organizational resilience against cyber threats

These results suggest that Saudi banks are actively working to strengthen their information security measures and develop comprehensive strategies to address social engineering risks.

- Challenges Hindering Knowledge Management in Countering Social Engineering:
  The study participants generally agreed on the challenges that impede the effective use of knowledge management in combating social engineering threats. However, their responses varied, with mean agreement scores ranging from 3.27 to 3.83, indicating that different challenges are perceived with varying degrees of importance.
- The key challenges identified include:
  - Lack of awareness among some employees regarding social engineering risks and countermeasures
  - Insufficient updates to internal security networks and management systems, leaving vulnerabilities unaddressed

These findings highlight the complex security challenges faced by Saudi banks and the need for continuous improvement in cybersecurity policies and practices.

Study Recommendations

Based on the study findings, the following recommendations are proposed:

1. Enhancing Awareness and Training:
   - Conduct regular training programs for banking sector employees on how to identify and respond to social engineering attacks.
   - Train staff to recognize common fraud tactics and deception methods used by cybercriminals.
2. Developing Effective Awareness Strategies:
   - Identify the most efficient methods for educating employees and customers in Saudi banks about social engineering risks.
   - Implement structured training programs that equip both employees and customers with practical knowledge on threat prevention.

DOI: 10.70000/cj.2024.74.616

3. Strengthening Security Policies and Procedures:
    - Establish a comprehensive security framework that includes well-defined policies and procedures to combat social engineering threats.
    - Ensure regular distribution and reinforcement of these policies among all employees.
4. Upgrading Security Technologies:
    - Periodically update security systems and fraud detection mechanisms to keep pace with emerging cyber threats.
    - Enhance identity verification technologies to prevent unauthorized access and fraudulent activities.
5. Expanding Awareness Initiatives for Employees and Customers:
    - Both employees and customers must be well-informed about social engineering tactics and equipped with practical skills to mitigate risks.
6. Strengthening Collaboration with Cybersecurity Authorities:
    - Establish continuous cooperation with relevant cybersecurity agencies to exchange critical information and stay updated on emerging threats.
    - Foster public-private partnerships to enhance cybersecurity resilience across the banking sector.

Future Research Directions

Based on the findings and recommendations of this study, the following future research topics are suggested:

1. Analyzing the Impact of Knowledge Management Strategies on Combating Social Engineering in Saudi Banks.
2. Investigating the Role of Advanced Technologies (e.g., Artificial Intelligence and Data Analytics) in Detecting and Preventing Social Engineering Attacks.
3. Reviewing the Existing Security Policies and Procedures in Saudi Banks and Their Effectiveness in Countering Social Engineering Threats.

DOI: 10.70000/cj.2024.74.616

4. Examining the Influence of Organizational Culture on Enhancing Awareness and Implementation of Security Measures Against Social Engineering.

These proposed studies will further contribute to the advancement of cybersecurity practices and enhance the resilience of Saudi banks against social engineering threats.

DOI: 10.70000/cj.2024.74.616