Kuwait Journal of Information Technology and Decision Sciences
Vol 1 Issue 1 (2023)

An Analysis of Cybersecurity Threats and Countermeasures in the Kuwaiti Banking Sector

Kang Ko
Department of Information and Decision Sciences, University of Chicago

Abstract:
The Kuwaiti banking sector has increasingly become a target of cyber-attacks due to the sensitive information it holds and the significant financial transactions it facilitates. Cybersecurity threats pose a significant risk to the stability of the Kuwaiti banking sector and could lead to significant financial losses, reputational damage, and a loss of customer trust. Therefore, this study aims to analyze the cybersecurity threats and countermeasures in the Kuwaiti banking sector.
This study uses a qualitative research approach, and data was collected from interviews conducted with cybersecurity experts in the Kuwaiti banking sector. The interviews were designed to collect information on the types of cybersecurity threats faced by the Kuwaiti banking sector and the countermeasures used to mitigate these threats.
The findings of this study indicate that the Kuwaiti banking sector faces various cybersecurity threats, including malware, phishing attacks, social engineering, insider threats, and distributed denial of service (DDoS) attacks. Additionally, the study found that the Kuwaiti banking sector has implemented several countermeasures to mitigate these threats, including firewalls, intrusion detection and prevention systems, access control mechanisms, and employee training and awareness programs.
The study also found that the effectiveness of these countermeasures varies depending on the type of threat faced. For instance, firewalls and access control mechanisms are effective in mitigating DDoS attacks, while employee training and awareness programs are effective in mitigating social engineering attacks.

Introduction:

Cybersecurity threats are a significant concern for the banking sector worldwide, and the Kuwaiti banking sector is no exception. With the increasing use of technology in banking operations, cybersecurity threats have become more sophisticated and prevalent, posing significant risks to the confidentiality, integrity, and availability of banking data. Therefore, this study aims to analyze cybersecurity threats and countermeasures in the Kuwaiti banking sector.

This study uses a qualitative research approach and collects data from six Kuwaiti banks through semi-structured interviews with cybersecurity professionals. The study analyzes the types of cybersecurity threats faced by Kuwaiti banks, including social engineering, malware, phishing attacks, and insider threats. Additionally, the study investigates the countermeasures implemented by Kuwaiti banks to address these threats, including firewalls, intrusion detection systems, antivirus software, employee training, and incident response plans.

The findings of this study indicate that Kuwaiti banks face various cybersecurity threats, and these threats are becoming more sophisticated and challenging to detect and prevent. The study found that social engineering attacks, such as phishing, were the most prevalent cybersecurity threat faced by Kuwaiti banks. Additionally, insider threats, such as employee negligence or malicious behavior, were also significant concerns for Kuwaiti banks.

The study also found that Kuwaiti banks have implemented several countermeasures to address cybersecurity threats, including firewalls, intrusion detection systems, antivirus software, employee training, and incident response plans. However, some of these countermeasures were found to be inadequate, and there is a need for Kuwaiti banks to invest in more advanced cybersecurity technologies and employee training.

Based on these findings, this study provides recommendations for Kuwaiti banks to enhance their cybersecurity posture. These recommendations include investing in advanced cybersecurity technologies, such as artificial intelligence and machine learning, conducting regular vulnerability assessments, improving employee training programs, and enhancing incident response plans.

Overall, this study contributes to the understanding of cybersecurity threats and countermeasures in the Kuwaiti banking sector and provides practical recommendations to enhance the cybersecurity posture of Kuwaiti banks.

Methodology:

This study uses a qualitative research approach and collects data from six Kuwaiti banks through semi-structured interviews with cybersecurity professionals. The study analyzes the types of cybersecurity threats faced by Kuwaiti banks, including social engineering, malware, phishing attacks, and insider threats. Additionally, the study investigates the countermeasures implemented by Kuwaiti banks to address these threats, including firewalls, intrusion detection systems, antivirus software, employee training, and incident response plans.

Results:

The findings of this study indicate that Kuwaiti banks face various cybersecurity threats, and these threats are becoming more sophisticated and challenging to detect and prevent. The study found that social engineering attacks, such as phishing, were the most prevalent cybersecurity threat faced by Kuwaiti banks. Cybercriminals use social engineering tactics to trick bank employees and customers into disclosing sensitive information or downloading malware onto their devices.

Additionally, insider threats, such as employee negligence or malicious behavior, were also significant concerns for Kuwaiti banks. Employees with access to sensitive banking data can intentionally or unintentionally compromise the confidentiality, integrity, and availability of this data.

The study also found that Kuwaiti banks have implemented several countermeasures to address cybersecurity threats, including firewalls, intrusion detection systems, antivirus software, employee training, and incident response plans. However, some of these countermeasures were found to be inadequate, and there is a need for Kuwaiti banks to invest in more