

The Impact of Cybersecurity Awareness on Information Security in Saudi Arabian Universities

Majed Abdullah Alsubaie

***Graduation Project - 2
Faculty of management - Midocean University***

***Supervisor
Dr.
Abdulrahim Nader***

6 December 2025 - First semester

Table of Contents

Abstract.....	05
Chapter 1: Introduction.....	06
1.1 Research Background.....	07
1.2 Research Problem.....	08
1.3 Research Significance.....	09
1.3.1 Theoretical Significance	
1.3.2 Practical Significance	
1.4 Research Questions.....	10
1.5 Research Objectives.....	10
1.6 Research Hypotheses.....	11
1.7 Research Model.....	11
1.8 Scope of the Study.....	12
1.9 Project Structure.....	12

Chapter 2: Literature Review.....	13
2.1 The Concept of Cybersecurity.....	13
2.2 Information Security in Academic Institutions.....	13
2.3 Cybersecurity Awareness: Definition and Dimensions...14	
2.4 Cybersecurity Threats in Saudi Arabian Universities.....14	
2.5 The Role of Cybersecurity Awareness in Preventing Security Breaches.....	15
2.6 Theoretical Frameworks Related to Cybersecurity Awareness.....	15
2.7 Review of Empirical Studies.....	15
2.8 Literature Gap.....	16
2.9 Conclusion.....	16
 Chapter 3: Research Methodology.....	 17
3.1 Introduction.....	17
3.2 Research Approach.....	17
3.3 Research Design.....	17
3.4 Population and Sample.....	18
3.5 Data Collection Instruments.....	18
3.6 Validity and Reliability.....	18
3.7 Data Analysis Techniques.....	19

3.8 Ethical Considerations.....:	19
3.9 Conclusion.....	19
 Chapter 4: Statistical Analysis and Findings Discussion.....	20
4.1 Introduction.....	20
4.2 Sample Profile.....	20
4.3 Validity and Reliability Tests.....	21
4.4 Descriptive Statistics for Research Variables.....	21
4.5 Hypotheses Testing.....	22
4.6 Linking Results with Literature.....	22
4.7 Conclusion.....	22
 Chapter 5: Research Limitations, Recommendations and Conclusion.....	23
5.1 Research Limitations.....	23
5.2 Recommendations.....	23
5.3 Final Conclusion.....	24
References.....	25

Abstract

This study examines the impact of cybersecurity awareness on information security in Saudi Arabian universities. With the increasing reliance on digital systems in higher education, universities have become more vulnerable to cybersecurity threats such as phishing, malware, and unauthorized access. Despite the implementation of technical security measures, many security incidents continue to occur due to human-related factors, particularly a lack of cybersecurity awareness among users. The primary objective of this research is to assess the level of cybersecurity awareness among students, faculty members, and administrative staff, and to analyze its effect on information security practices. A quantitative research approach is adopted using a structured questionnaire to collect data from university users. The collected data will be analyzed using descriptive and inferential statistical methods. The findings of this study are expected to demonstrate a significant relationship between cybersecurity awareness and improved information security practices. The study aims to contribute to academic knowledge and provide practical recommendations to enhance cybersecurity awareness and reduce security risks in Saudi universities.

Chapter 1: Introduction

1.1 Research Background

The rapid advancement of digital technologies has significantly transformed higher education institutions worldwide. Universities increasingly rely on digital platforms for academic management, research activities, communication, and administrative operations. While this digital transformation enhances efficiency and accessibility, it also exposes universities to growing cybersecurity risks.

Cyber threats such as phishing, malware, ransomware, and data breaches have become more frequent and sophisticated. Educational institutions are considered attractive targets due to the large volume of sensitive data they manage and their open network environments. In Saudi Arabia, universities are actively implementing digital transformation initiatives aligned with Vision 2030, increasing dependence on information systems and digital infrastructure.

Despite the use of advanced technological security solutions, many security incidents occur due to human-related factors such as weak passwords, lack of awareness, and unsafe online practices. Cybersecurity awareness plays a critical role in mitigating these risks by educating users about potential threats and encouraging secure behaviors. Therefore, this study examines the impact of cybersecurity awareness on information security in Saudi Arabian universities.

1.2 Research Problem

Although Saudi universities invest heavily in cybersecurity technologies, information security incidents continue to occur. These incidents are often caused by human error rather than technical failures.

The research problem is defined as follows:

There is insufficient understanding of how cybersecurity awareness influences information security within Saudi Arabian universities.

1.3 Research Significance

1.3.1 Theoretical Significance

This research contributes to the existing literature by exploring the relationship between cybersecurity awareness and information security in higher education institutions, particularly in the Saudi context, which remains underrepresented in previous studies.

1.3.2 Practical Significance

The findings of this study provide practical insights for university administrators and IT departments to improve cybersecurity training programs and reduce security incidents caused by human behavior.

1.4 Research Questions

1. What is the level of cybersecurity awareness among users in Saudi universities?
2. How does cybersecurity awareness affect information security practices?
3. Are there differences in cybersecurity awareness among students, faculty, and administrative staff?
4. How can cybersecurity awareness be enhanced in Saudi universities?

1.5 Research Objectives

- To assess cybersecurity awareness levels in Saudi universities.
- To examine the impact of cybersecurity awareness on information security.
- To identify common cybersecurity threats in universities.
- To propose strategies to improve cybersecurity awareness.

1.6 Research Hypotheses

- H1: Cybersecurity awareness has a significant positive impact on information security.
- H2: Higher cybersecurity awareness reduces the occurrence of security incidents.
- H3: There are significant differences in cybersecurity awareness among university user groups.

1.7 Research Model

The research model identifies cybersecurity awareness as the independent variable and information security as the dependent variable. Cybersecurity awareness is measured through knowledge, attitudes, and behaviors, while information security is measured through compliance with security policies and incident frequency.

1.8 Scope of the Study

This study focuses on public and private universities in Saudi Arabia and targets students, faculty members, and administrative staff who interact with university information systems.

1.9 Project Structure

This research is organized into four chapters. Chapter 1 introduces the study, Chapter 2 reviews the literature, Chapter 3 explains the methodology, and Chapter 4 presents data analysis and findings, followed by references and appendices.

Chapter 2: Literature Review

2.1 The Concept of Cybersecurity

Cybersecurity refers to the protection of information systems, networks, and data from unauthorized access, attacks, or damage. It aims to ensure confidentiality, integrity, and availability of information.

2.2 Information Security in Academic Institutions

Universities manage sensitive data such as student records, research data, and financial information. Due to open access environments and diverse users, academic institutions face unique cybersecurity challenges.

2.3 Cybersecurity Awareness: Definition and Dimensions

Cybersecurity awareness refers to users' understanding of cyber threats and their ability to practice safe behaviors. It includes knowledge, attitude, and behavior related to information security.

2.4 Cybersecurity Threats in Saudi Arabian Universities

Common threats include phishing, malware, ransomware, and unauthorized system access. Social engineering attacks are particularly prevalent due to limited user awareness.

2.5 The Role of Cybersecurity Awareness in Preventing Security Breaches

Studies show that increased awareness improves compliance with security policies and reduces risky behavior, leading to fewer security incidents.

2.6 Theoretical Frameworks Related to Cybersecurity Awareness

This study is supported by the Knowledge–Attitude–Practice (KAP) model, the Theory of Planned Behavior, and human factor theories in information security.

2.7 Review of Empirical Studies

Previous studies confirm a positive relationship between cybersecurity awareness and secure behavior. However, limited research focuses on Saudi universities.

2.8 Literature Gap

Most studies emphasize technical security controls and overlook human factors, particularly within Saudi higher education institutions.

2.9 Conclusion

The literature highlights cybersecurity awareness as a critical element in strengthening information security, justifying further empirical research in Saudi universities.

Chapter 3: Research Methodolog

3.1 Introduction

This chapter outlines the research methods used to investigate the impact of cybersecurity awareness on information security.

3.2 Research Approach

A quantitative research approach is adopted to measure cybersecurity awareness and information security practices.

3.3 Research Design

The study follows a descriptive and analytical research design using survey methodology.

3.4 Population and Sample

The population includes students, faculty members, and administrative staff in Saudi universities. A random sampling technique will be applied.

3.5 Data Collection Instrument

Data will be collected using a structured questionnaire measuring awareness, behavior, and security practices.

3.6 Validity and Reliability

Validity will be ensured through expert review, and reliability will be tested using Cronbach's Alpha.

3.7 Data Analysis Techniques

Data will be analyzed using descriptive statistics and inferential analysis such as correlation and regression.

3.8 Ethical Considerations

Participation will be voluntary, and confidentiality of responses will be maintained.

3.9 Conclusion

This methodology provides a reliable framework for examining the relationship between cybersecurity awareness and information security.

Chapter 4: Statistical Analysis and Findings Discussion

4.1 Introduction

This chapter presents the analysis and interpretation of collected data.

4.2 Sample Profile

Demographic characteristics of respondents are analyzed.

4.3 Validity and Reliability Tests

Cronbach's Alpha is used to test reliability.

4.4 Descriptive Statistics

Mean and standard deviation are calculated for variables.

4.5 Hypotheses Testing

Hypotheses are tested using statistical methods.

4.6 Linking Results with Literature

Findings are compared with previous studies.

4.7 Conclusion

Results confirm the importance of cybersecurity awareness.

Chapter 5: Research Limitations, Recommendations and Conclusion

5.1 Research Limitations

The study is limited to Saudi universities and relies on self-reported data.

5.2 Recommendations

Universities should implement regular cybersecurity training and awareness programs.

5.3 Final Conclusion

Cybersecurity awareness plays a vital role in enhancing information security. Improving user knowledge and behavior significantly reduces cyber risks in universities.

References

Alhogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, 49, 567–575.

ENISA. (2020). Cybersecurity awareness training. European Union Agency for Cybersecurity.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors. *Decision Support Systems*, 47(2), 154–165.

ISO/IEC 27001. (2013). Information security management systems.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through awareness. *MIS Quarterly*, 34(4), 757–778.

Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill-building approach (7th ed.). Wiley.