

Research Issues

RSC811-Assignment 4

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

The title, "**Cybersecurity Enterprises Policies: A Comparative Study**", is relevant and engaging, as it addresses a critical area of cybersecurity policy across multiple industries.

The topic is timely and important, especially as enterprises invest heavily in cybersecurity policies to protect their digital assets.

The title could be slightly more precise, indicating the specific industries examined in the study (healthcare, finance, education, aviation, and e-commerce).

Introduction : المقدمة

The introduction provides a strong background on cybersecurity policies and their importance for businesses.

It clearly outlines the research context, explaining why comparing cybersecurity policies across different industries is necessary.

The introduction successfully summarizes the study's scope but does not explicitly define the independent, dependent, moderator, or mediator variables.

Problem Statement : مشكلة الدراسة

The paper identifies a gap in cybersecurity research: the lack of understanding of common security policies across industries.

The research problem is framed as two research questions

RQ1 What are the aspects of cybersecurity that different enterprises have in common?

RQ2: How are the cybersecurity aspects used among different enterprises?

focusing on common cybersecurity aspects and their implementation in enterprises.

While the study acknowledges gaps in prior research, it does not explicitly discuss how it builds upon past limitations in cybersecurity policy studies.

Part

4

أهمية الدراسة : Importance of the Study

The study contributes theoretically by consolidating cybersecurity policy aspects across multiple industries.

It provides practical insights for policymakers and decision-makers by identifying the most crucial security policies per industry.

However, the paper could better highlight how organizations can directly implement these findings in real-world cybersecurity frameworks.

Part

5

Objectives of the Study : أهداف الدراسة

Objectives:

The study aims to identify and compare 10 common cybersecurity policy aspects across five industries.

The objectives align well with the research questions but lack explicit discussion on how realistic they are to achieve.

Concepts and Definitions : مفاهيم وتعريفات الدراسة

The paper discusses key cybersecurity policy aspects such as privacy, website security, cloud security, email security, physical security, network security, information security, access control, data retention, and data protection.

While the variables are defined, their relationships (e.g., cause-effect between independent and dependent variables) are not explicitly modeled.

Part

7

الدراسات السابقة - Previous Studies

The literature review is comprehensive, covering various cybersecurity policies, regulatory frameworks, and industry-specific security measures. However, it does not include a direct comparison of its findings with previous studies to highlight new contributions.

Part

8

Hypotheses : فرضيات الدراسة

The study does not explicitly state hypotheses but instead focuses on research questions (RQ1 & RQ2).

Including hypotheses would strengthen the study by providing testable predictions regarding cybersecurity policy implementation.

Study Model : نموذج الدراسة

There is no formal conceptual model, but the study presents a taxonomy of cybersecurity policies in different enterprises. A visual framework illustrating how these policies interact across industries would enhance clarity.

Methodology and Statistical Analysis: منهجية الدراسة و التحليل الاحصائي

The study relies on a systematic literature review rather than primary data collection.

It synthesizes data from academic papers and corporate reports but lacks empirical validation through surveys or case studies.

Future research could benefit from statistical analysis of cybersecurity policy effectiveness in real-world organizations.

Discussion of Results and Recommendations : مناقشة النتائج والتوصيات

The discussion connects findings with previous literature and highlights the varying importance of security policies across industries.

Practical recommendations include implementing industry-specific cybersecurity policies and creating dedicated cybersecurity teams within organizations.

The study acknowledges its limitations, such as focusing on only five industries and relying solely on literature reviews.

Future research directions include expanding the study to more industries and conducting fieldwork for empirical validation.

Part

12

Overall Assessments :

Strengths:

Relevant and engaging research area

Well-structured comparison of cybersecurity policies across industries

Comprehensive literature review

Practical recommendations for enterprises

Areas for Improvement:

Clearly define variables and relationships in a conceptual framework

Include hypotheses to test cybersecurity policy impacts

Use empirical methods (e.g., surveys, case studies) for validation

Provide more direct comparisons with past research findings

Article link :

<https://www.mdpi.com/1424-8220/22/2/538/pdf?version=1641902563>