

Research Issues

RSC811-Assignment 9

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

The Article: "Cyber Governance Studies in Ensuring Cybersecurity"

Engaging Field: The title reflects a highly relevant and timely topic, given the global rise in cyber threats.

Clarity of Variables: Since the paper is conceptual, it does not define variables in the traditional quantitative sense (i.e., independent, dependent, mediating, moderating). However, it discusses key constructs such as cybersecurity strategy, leadership, and compliance.

Scope of Application: The application context is broadly organizational; no specific industry is targeted, though examples span multiple sectors like healthcare and critical infrastructure.

Introduction : المقدمة

The introduction highlights:

The growing threat of cybersecurity incidents.

The shift toward enterprise-wide responsibility for cybersecurity.

The need for better governance mechanisms.

It does not outline study variables in a concise or structured manner, as a quantitative study would, but effectively sets the stage for the conceptual model.

Part

3

Problem Statement : مشكلة الدراسة

The study identifies a clear gap in literature: the lack of an integrated model showing how key components like leadership, strategy, and compliance interact to form effective cybersecurity governance.

The authors discuss this as a research gap but do not pose specific research questions or hypotheses, since the study is conceptual and theoretical in nature.

أهمية الدراسة : Significance of the Study

Theoretical Contribution: It contributes a conceptual foundation for further theory development and empirical testing in cybersecurity governance.

Practical Relevance: The model has practical value for decision-makers, emphasizing strategy alignment, cultural factors, and leadership oversight—elements critical for implementation.

It offers practical insights and recommendations, such as involving top management and enhancing employee awareness.

Part

5

أهداف الدراسة : Objectives of the Study

The main objective is to develop a comprehensive conceptual model for cybersecurity governance.

The goal is feasible and relevant, though not empirically tested.

The objectives align well with the problem and literature gap.

Concepts and Definitions : مفاهيم وتعريفات الدراسة

Key concepts are clearly defined and well-supported with references:

Cybersecurity strategy

Leadership and oversight

Organizational culture

Compliance and accountability

The paper provides a logical framework and links these concepts to governance.

Sub-dimensions are identified (e.g., types of cybersecurity, risk appetite, KPI development), and the justification for including them is well-explained.

Part

7

الدراسات السابقة: Literature review

The literature review is rich and well-integrated.

It draws on recent sources (mostly 2016–2020) and engages critically with existing work.

Highlights both areas of consensus and gaps.

The review supports the development of the conceptual framework and could be used to formulate future hypotheses.

Hypotheses : فرضيات الدراسة

The study does not include formal hypotheses as it is not empirical.

However, the model provides a foundation for future research hypotheses, such as:

The impact of leadership on cybersecurity policy adherence.

The relationship between resource availability and governance effectiveness.

Study Model : نموذج الدراسة

A conceptual model is presented (Figure 2).It clearly illustrates relationships among the five core components:

Cybersecurity Strategy
Standardized Processes
Compliance and Accountability
Senior Leadership Oversight
Resources

The model is visually clear and logically coherent, though not empirically tested.

Methodology and Statistical Analysis: منهجية الدراسة و التحليل الاحصائي

Nature of Study: The research is theoretical and conceptual.

No data collection or statistical analysis was conducted.

No sampling, instruments, or quantitative techniques were used.

The methodology relies on synthesis of existing literature and logical reasoning.

Discussion of Results and Recommendations : مناقشة النتائج والتوصيات

The discussion connects well with existing literature and highlights:

The importance of cultural and human factors in cybersecurity.

The need for leadership engagement and continuous training.

The challenge of policy non-compliance and how to address it.

Recommendations are practical and grounded in literature.

The paper suggests the model can be tested in future empirical research and adapted to specific contexts.

It also proposes future research directions focused on empirical validation.

Part

12

Overall Assessments :

The paper successfully identifies a conceptual gap and proposes a detailed model.

Emphasizes the role of human behavior, leadership, and culture.

Makes both theoretical and practical contributions.

Lays a strong foundation for future empirical studies and policy development.

Article link :

https://www.researchgate.net/profile/Salifu-Yusif-2/publication/351508606_A_Conceptual_Model_for_Cybersecurity_Governance/links/60b2046292851cd0d980e3ec/A-Conceptual-Model-for-Cybersecurity-Governance.pdf