

Literary Criticism RCS813 - Assignment 8

Prepared by
Abdulaziz Alarfaj



Part
01

Research Title

Assignment : Critique of Research Paper in Terms of
Results and recommendations

Article Chosen :

A Conceptual Model for Cybersecurity Governance

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

Published in 2021

Part 01

Research Title

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.

1. Alignment with Existing Literature:

The authors highlight how the proposed model is grounded in and supported by current literature on cybersecurity, leadership, organizational behavior, and compliance.

They reference several case examples and statistics (e.g., Equifax, WannaCry, Target breach) to emphasize the real-world significance of human factors, weak leadership oversight, and fragmented policies.

2. Practical Recommendations:

Engage top-level leadership to champion and sustain cybersecurity efforts.

Develop context-specific policies and training programs rather than one-size-fits-all solutions.

Embed cybersecurity into organizational culture through continuous awareness and behavior change.

Conduct regular evaluations and updates of security strategies to adapt to emerging threats.

3. Actionable Value:

The paper presents the model as a blueprint for decision-makers, especially CISOs, CIOs, and senior executives, to build or improve governance programs. While it does not provide specific tools, it encourages organizations to build their programs around the model's components.

4. Future Research Directions:

Future Research Directions: The authors propose empirical validation of the model in different sectors and organizational contexts. They suggest that future research should test the model using surveys, case studies, or mixed methods to assess its impact on compliance and incident reduction.

5. Summary

The discussion effectively argues that cybersecurity governance must evolve from a compliance-based mindset to a strategic, integrated organizational function.

The model is positioned not just as a theoretical contribution but as a practical guide that organizations can adapt and build upon.