

Literary Criticism RCS813 - Assignment 6

Prepared by
Abdulaziz Alarfaj



Part
01

Research Title

Assignment : Critique of Research Paper in Terms of
Research Importance

Article Chosen :

The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities

<https://www.sce.carleton.ca/faculty/wainer/papers/1-s2.0-S0268401222000548-main.pdf>

Published in 2022

1. Addressing a Growing Global Challenge

Cybersecurity is a growing concern across industries due to increasing cyber threats, especially in the context of global supply chains that are becoming more interconnected and dependent on digital technologies. The paper highlights how vulnerabilities in cybersecurity can directly affect the stability and integrity of entire supply chains. By bringing attention to these risks, it contributes to the broader conversation about securing digital infrastructure in the modern world.

2. Linking Human Behavior to Cybersecurity Resilience

Many cybersecurity discussions focus on technical solutions (e.g., firewalls, encryption, and security software). However, this paper emphasizes the often-overlooked role of human behavior in maintaining cybersecurity. Employee awareness, attitudes, and compliance with policies are crucial for preventing breaches. By exploring this relationship, the paper sheds light on how employee engagement and a strong security culture can be as important as technical measures, offering a more holistic approach to cybersecurity.

3. Enhancing Understanding of Compliance Dynamics

The paper brings clarity to the often-complicated dynamics of employee compliance with cybersecurity policies. It provides a framework for understanding how and why employees comply (or fail to comply) with these policies, and how organizations can better foster compliance through training, communication, and leadership. This contributes to a more nuanced understanding of what drives or hinders compliance, making it an invaluable resource for both academics and practitioners.

4. Relevance to Small and Medium-Sized Enterprises (SMEs)

Smaller businesses often lack the resources or expertise to implement comprehensive cybersecurity programs. This paper's focus on SMEs is highly relevant, as it provides actionable insights on how these businesses can improve their cybersecurity posture without needing vast financial investments. It emphasizes the importance of building a security-conscious workforce, which is a more cost-effective strategy than investing heavily in technology alone.

5. Policy Implications

The paper also provides valuable insights into how organizations can develop better cybersecurity policies, with a focus on making these policies clear, accessible, and effective. It encourages organizations to take a more strategic approach to policy development by considering employee understanding and engagement. This is important not just for individual companies but for broader policy development and governance at the industry or national level.

6. Timely Contribution in the Post-Pandemic Era

The COVID-19 pandemic accelerated the digital transformation of businesses and highlighted the vulnerabilities of supply chains. Cybersecurity threats have become more sophisticated during this time. This paper is particularly important in the post-pandemic context, offering relevant solutions to address the new challenges organizations face in maintaining secure and resilient supply chains.

Conclusion

In essence, the overall importance of the paper lies in its ability to bridge technical, human, and organizational aspects of cybersecurity. It provides a comprehensive perspective on how employee attitudes, behavior, and awareness can significantly enhance an organization's cybersecurity defenses, contributing to the broader goal of building resilient supply chains. Its insights are especially valuable in today's increasingly digital world, where the security of supply chains is critical to business continuity and economic stability.