

Research Skills RSC777

Task 2

Prepared by
Abdulaziz Alarfaj



Part

1

Research Title : العنوان

"The research paper

"Cybersecurity Enterprises Policies: A Comparative Study"

Article link :

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

Why This Introduction Was Chosen

1. Clear Definition of Scope:

The author begins by defining cybersecurity not only as a technical field but also as an area encompassing organizational, governance, and policy dimensions. This broad framing immediately situates the study within the interdisciplinary nature of cybersecurity research an essential quality for a policy-focused study.

2. Establishes Relevance and Importance: The introduction effectively highlights why cybersecurity matters today: it connects the concept to global digital interdependence and the growing exposure to cyber threats. By emphasizing the social and organizational impact rather than purely technical aspects, the author underscores the real-world significance of the topic.

Why This Introduction Was Chosen

3. Contextual Link to Policy Frameworks: It narrows down from the general problem of cybersecurity to the specific concern of policy frameworks and their role in ensuring interoperability and data protection. This progression from broad to specific follows a logical academic flow and prepares the reader for the study's focus on governance mechanisms.

4. Balanced Technical and Policy Perspective: Unlike many technical papers that start with attack vectors or system vulnerabilities, this introduction integrates both technological and regulatory contexts. That balance reflects how cybersecurity has evolved from an IT issue to a core element of national policy and international cooperation.

مشكلة بحثية في حدود 500 كلمة

The rapid digitalization of government and industry has intensified exposure to cybersecurity threats. While technological countermeasures have advanced significantly, the ultimate defense of a nation's digital ecosystem depends on effective public policy and regulatory governance. Policymakers have responded by introducing comprehensive frameworks such as the European NIS2 Directive, the United States Cybersecurity Framework 2.0, and Saudi Arabia's National Cybersecurity Authority (NCA) Essential Cybersecurity Controls, which establish baseline requirements for risk management, incident reporting, and supply chain protection. However, despite these initiatives, empirical evidence on the actual impact of such policies remains limited and fragmented. Many studies describe the content of cybersecurity policies but rarely measure their influence on organizational cybersecurity maturity or the frequency and severity of incidents. In addition, regulations vary considerably across jurisdictions, creating compliance challenges for multinational organizations and uncertainty for smaller enterprises that lack the resources to interpret and implement multiple overlapping requirements. Another challenge lies in balancing regulatory rigor with innovation. Excessive or poorly coordinated regulation may hinder technological progress, particularly among start-ups and open-source communities, while overly flexible frameworks can lead to inconsistent enforcement and continued vulnerabilities. There is also a geographic and contextual bias in existing research, as most empirical analyses originate from developed economies. This has left significant gaps in understanding how cybersecurity policies operate in developing or resource-constrained environments. Therefore, there is an urgent need for research that systematically evaluates the effectiveness and contextual adaptability of cybersecurity-related public policies. Such research should determine which policy mechanisms—such as mandatory reporting, certification schemes, incentives, or penalties—produce measurable improvements in resilience. It should also explore how organizations perceive and respond to regulatory requirements and whether these policies foster a genuine culture of security or only procedural compliance. This study addresses the central problem of the lack of a unified, evidence-based understanding of how cybersecurity-related public policies influence organizational readiness and national cyber resilience. By examining this issue across different policy environments and organizational contexts, the research aims to contribute to the development of more effective and context-sensitive cybersecurity governance models that align legal requirements with operational realities.

Part

3

ما الذي يتم اخذه بعين الاعتبار

Start broad, then narrow: Begin with a global or societal issue and gradually focus on your specific research gap.

Establish significance: Explain why the topic matters academically, practically, or socially.

Show the gap: Clearly state what is missing in current knowledge or practice.

State the aim/objectives: Specify what the study will accomplish.