Strategic Risk Management in the Cyber Threat Era: The Impact of Information Security Governance on Competitive Advantage

Bondan Haryono [1], **Galih Wahid Hasyim** [2], **Edwin Julianus Sebayang** [3], **Dwi Handoko** [4]

[134] Faculty Of Economics And Business, Universitas Trisakti, Indonesia
[2] Human Resource Development Agency Defense, Ministry Defense of the Republic Indonesia, Indonesia

https://doi.org/10.35609/gcbssproceeding.2026.1(12)

ABSTRACT

The global business landscape is currently undergoing a fundamental transformation driven by the massive integration of digital technologies across organizational value chains. However, this accelerated digitalization brings a paradoxical consequence: while it enhances operational efficiency, it simultaneously expands the "attack surface" for increasingly sophisticated cyber threats. Cyber threats are no longer merely technical disruptions to IT infrastructure; they have evolved into existential risks capable of paralyzing entire business strategies. Consequently, organizations are compelled to shift their risk management paradigm from a reactive-operational approach toward Strategic Risk Management (SRM) that is proactive and integrated with the company's long-term objectives. In a highly competitive market, digital resilience is now viewed as a new source of Competitive Advantage, fostering higher levels of digital trust among stakeholders, particularly customers and investors. Despite the widely recognized urgency of cybersecurity, a critical research problem persists: many organizations remain trapped in "siloed" governance models that focus strictly on technical compliance. The effectiveness of information asset protection depends heavily on the extent to which Information Security Governance (ISG) is internalized within leadership structures and organizational culture. Without a mature governance framework, cyber vulnerabilities can lead to significant financial losses, brand reputation damage, and the loss of intellectual property. This issue is further compounded by a distinct research gap in current literature; prior studies have predominantly focused on technical aspects, such as encryption or intrusion detection, without empirically linking them to an organization’s dynamic capability to respond to strategic threats. Therefore, this article aims to bridge this gap by analyzing the influence of information security governance on competitive advantage within a strategic risk management framework to build competitive cyber resilience.

JEL Codes:

Keywords: *Strategic Risk Management, Information Security Governance, Competitive Advantage, Cyber Threats, Digital Trust*