GOVERNANCE OF CYBERSECURITY COMPANIES IN COMBATING CYBERCRIME

Muaath S. Al-Mulla *, Mariam H. Al Dhubaiee *

* Kuwait International Law School (KILAW), Doha, Kuwait

OPEN ACCESS

How to cite: Al-Mulla, M. S., & Al Dhubaiee, M. H. (2024). Governance of cybersecurity companies in combating cybercrime. In Ž. Stankevičiūtė, A. Kostyuk, M. Venuti, & P. Ulrich (Eds.), *Corporate governance: Research and advanced practices* (pp. 139–141). Virtus Interpress. https://doi.org/10.22495/cgrapp25

Received: 01.05.2024
Accepted: 21.05.2024
Keywords: Principles of Governance, Cybersecurity, Companies, Cyber Risks, Compliance with Safety Rules, Forecasting and Preventive Measures
JEL Classification: K220, K240, K290, K420
DOI: 10.22495/cgrapp25

Abstract

This research study aims to analyze the policies, procedures, and processes adopted by cybersecurity companies for managing and predicting cyber risks and combating cybercrimes. To achieve the research objective the inductive approach. The study concludes that government laws are no longer able to confront cyber threats without the private sector's participation, specifically cybersecurity companies, and investment therein, and the adoption of governance policy by those companies may obtain reasonable flexibility in preventing cybercrimes.

1. INTRODUCTION

Companies heavily depend on modern technology in conducting their various transactions. Given their fundamental role in building communities in all fields, the enhanced role of those companies in the prevention of risks, especially in the cyber environment is undeniable.

The topic of this research is particularly significant in understanding the policies, procedures, and processes adopted by cybersecurity companies under the concept of governance, establishing

a general framework for managing and predicting risks and compliance in the cyber environment in line with cybercrime prevention issues and the extent of its flexibility in contributing to building partnerships between government agencies and civil society. Investing in cybersecurity companies is one of the issues that enhances the stability of the general cybersecurity situation and even boosts confidence among those dealing with this environment, which may be observed in the huge amounts spent to develop that system.

Government laws are no longer able to confront cyber threats, especially after they developed their methods and the high cost of the losses they cause, to the point that investing in cybersecurity, to combat cybercrimes, has become a necessity and not just an option. Therefore, this research tackles several questions:

RQ1: What is the volume of cyber threats at present?

RQ2: Do cybersecurity companies undertake a key role in preventing cybercrimes?

RQ3: To what extent governance policies can manage cyber risk prevention mechanisms and predict them?

2. METHODOLOGY

An inductive approach is adopted in presenting this study to achieve the objective intended therefrom. Hence, several questions were raised based on the solutions provided by cybersecurity companies that rely on governance policy in organizing and managing risks and compliance as mechanisms for cybercrime prevention and those mechanisms' success in reducing their impacts. Under that methodology, we divided the plan into several requirements: the First Requirement explains the basic concepts of research, the Second Requirement tackles the key and volume of cyber threat risks, and the Third Requirement indicates the significant role of cybersecurity companies in confronting those threats and the extent of the governance policy's success in risks management and prediction.

3. CONCLUSION

The research concludes with several crucial results that demonstrate the inability of governments and civil society to confront cybercrimes without the private sector's participation, specifically cybersecurity companies, and investment therein. It is also found that the adoption of governance policy by those companies may achieve sufficient flexibility in cybercrime prevention.

REFERENCES

Bin Issa, L., & Zamora, J. (2022). 'Ahamiyat hawkamat al'amn alsaybiranii lidaman tahawul raqamayin amin lilkhidma aleumumiat fi aljazayir [Importance of cybersecurity governance for ensuring a secure digital transformation of the public services in Algeria]. *Algeria Scientific Journal Platform, 7*(2), 414–429. https://www.asjp.cerist.dz/en/article/203547

Eitel, M. (2023, August 2). Corporate responsibility in the age of AI. *Project Syndicate*. https://www.project-syndicate.org/commentary/ai-regulation-corporate-responsibility-action-plans-by-maria-eitel-2023-08

Iannone, P., & Omar, A. (2016). *Cybersecurity governance: Five reasons your cybersecurity governance strategy may be flawed and how to fix it*. Kogod School of Business, American University. https://outsourcing.com/cybersecurity-governance-five-reasons-your-strategy-may-be-flawed-and-how-to-fix-it/

Le Centre Pour La Gouvernance Du Secteur De La Sécurité, Genève (DCAF). (2019). *Guide to good governance in cybersecurity*. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021.pdf

Léger, M.-A. (2023). Gouvernance de la cybersécurité [Cybersecurity governance]. In *Introduction à la gouvernance de la cybersécurité pour la gestion des technologies d'affaires* [Introduction to cybersecurity governance for business technology management] https://www.researchgate.net/publication/371363804_Introduction_to_Cybersecurity_Governance_for_Business_Technology_Management_Chapter_2_Cybersecurity_governance

McGrath, V., Sheedy, E. A., & Yu, F. (2022). *Governance of cyber security: State of play*. https://doi.org/10.2139/ssrn.3971177

Saja Fadel Abbas, M. M. (2024). Digital governance in light of cybersecurity threats: The UAE as a model. *Hammurabi Journal for Studies, 13*(49), 323–338. https://doi.org/10.61884/hjs.v13i49.445

Schjølberg, S., & Ghernaouti-Hélie, S. (2009). *A global protocol on cybersecurity and cybercrime: An initiative for peace and security in cyberspace*. Cybercrimedata. https://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf

Sharma, U. (2023). Strategies and challenges in combating cybercrime: A comprehensive analysis of cybersecurity technologies, legal frameworks, and preventative measures. *China Petroleum Processing and Petrochemical Technology, 23*(2), 4630–4642. https://zgsyjgysyhgjs.cn/index.php/reric/article/pdf/02-4630.pdf

van Eeten, M. J. G., De Bruijn, H., Kars, M., & Van Der Voort, H., & Van Till, J. (2006). The governance of cybersecurity: A framework for policy. *International Journal of Critical Infrastructures, 2*(4), https://doi.org/10.1504/IJCIS.2006.011345