SemeAd 2023
XXVI Seminários em Administração

07, 08, 09 e 10 de novembro de 2023
ISSN 2177-3866

Dynamic Capabilities in Cybersecurity: empirical evidence to enhance protection against cyber threats

ANGELICA PIGOLA
UNIVERSIDADE NOVE DE JULHO (UNINOVE)

PRISCILA REZENDE DA COSTA
UNIVERSIDADE NOVE DE JULHO (UNINOVE)

Agradecimento à orgão de fomento:
“This work was supported by Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES), grant number 001”.

Dynamic Capabilities in Cybersecurity: empirical evidence to enhance protection against cyber threats

Introdução

Fraud, malicious actions, cyber-attacks are a truly global problem affecting firms in different regions and industries worldwide. Measuring the true extent of the damage caused by these criminals disturbs to define what extent cybersecurity intelligence (CI) may protect a firm is challenger, due to the inherent nature of concealment involved in most schemes of cyber-criminal articulations. Cybersecurity risks demands for firms high efforts in developing innovations, technical process, and abilities to attain preventative strategies as referred in the literature of CI.

Problema de Pesquisa e Objetivo

Excessive information security may negatively impact a firm’s competitive advantage. It uncurtains others impacts such as on brand, crisis communication, business resumption, employees and public perception, customers retention, additional costs, third-party risks, firms' evaluation, among others. Thus, having a balanced approach requires a high level of capabilities to keep cybersecurity as a business enabler. Considering this scenario, many capabilities models have been subject to criticism because lack empirical foundation, oversimplify business reality, and not demonstrate their purpose.

Fundamentação Teórica

This research investigates the influence of dynamic capabilities in cybersecurity (DCCI) in cybersecurity intelligence (CI) bringing fraud diamond and dynamic capabilities theories to identify the capabilities to cybersecurity innovations (new technologies and processes implemented), organizational change (controls proactively implemented before a cyber-attack happens), and performance (new security threat-actors identified highlighting gaps in the firm's cyber defenses).

Metodologia

The dynamic capabilities on cybersecurity framework is built from a literature review of 47 case studies and tested as of 207 cybersecurity experts spread out in different regions and countries through hierarchical regressions.

Análise dos Resultados

The DDCI framework is positively associated with CI two different dimensions, Doing and Improving cybersecurity activities while the dimensions Enabling and Managing cybersecurity activities do not present significant impacting in CI.

Conclusão

To the best of the authors’ knowledge, this is the first paper that build an empirical instrument to measure a model of dynamic capabilities in cybersecurity intelligence. Findings expand on the perception of CI as multidimensional problems involving firms' innovations and change in information security field. Thus, it progresses to offer new avenues for future research and practice in building DCCI to enhance CI for business and society.

Referências Bibliográficas

Al-Matouq H, Mahmood S, Alshayeb M, Niazi M (2020) A Maturity Model for Secure Software Design: A Multivocal Study. IEEE Access 8:215758–215776. Al-Matari OMM, Helal IMA, Mazen SA, Elhennawy S (2021) Adopting security maturity model to the organizations’ capability model. Egyptian Informatics Journal 22:193–199. Steininger DM, Mikalef P, Pateli A, Ortiz-de-Guinea A

(2022) Dynamic Capabilities in Information Systems Research: A Critical Review, Synthesis of Current Knowledge, and Recommendations for Future Research. JAIS 22:447–490.