

An Interdisciplinary Study of Cybersecurity Investment in the Nonprofit Sector

Natalia Ermicioi
Marymount University

Xiang Michelle Liu
Marymount University

Cybersecurity is becoming a worldwide priority. It is critical for organizations to quantify losses from cybercrimes and make informed decisions on cybersecurity investments. This paper expands the body of knowledge in cybersecurity of nonprofit organizations (NPOs)—a less-researched area—by examining investment in NPOs’ cybersecurity from the business and economics perspectives. The authors combine two economics and risk management models to quantify the potential loss caused by a cyberattack. The paper provides a hypothetical example of applying the insights from the GL and FAIR risk models to assess the information assets of an NPO and calculating the optimal level of cybersecurity investment. Developing cybersecurity measures for NPOs is equally important as developing cybersecurity strategies, tools, and policies for large corporations or small businesses. Therefore, the findings of this paper can serve as decision-making tools for NPOs to evaluate information security assets, estimate the potential loss caused by cyberattacks, and determine the optimal investment value in cybersecurity measures.

Keywords: cybersecurity, nonprofit, risk management, investment

BACKGROUND

One of the latest McAfee reports revealed that the annual monetary loss from cybercrime would create a \$1 trillion drag on the global economy in 2020 (Malekos & Lostri, 2020). As ransomware and phishing campaigns are skyrocketing (Verizon, 2021), the cost of global cybercrime is expected to continue increasing and to reach \$10.5 trillion annually by 2025 (Morgan, 2020). To achieve such a level of growth, cybercrime has been organized like a business, spread and delivered through supply chains, services, and distribution channels. As cyber threats have evolved from targeting and harming computers, networks, and smartphones to affecting people, cars, gas pipelines, and medical devices, businesses of all sizes and in all sectors including healthcare organizations, schools, and local governments, could be cybercriminal group targets. The recent President Executive Order (EO) on “Improving the Nation’s Cybersecurity” reflects the national security implications of cybersecurity attacks on everyday life (Executive Office of the President, 2021). Therefore, it is critical for organizations to understand the factors involved in quantifying losses from cybercrime as well as costs of cybersecurity investment in order to make informed decisions on cybersecurity spending and reduce risks from cyberattacks (AT&T, 2017; Gordon et al., 2015).