Article Review #2: Revealing the Realities of Cybercrime in Small and Medium Enterprises

Khamari Phillips

Cybersecurity, Old Dominion University

CRN 20932: CYSE 201S

Professor Yalpi

November 7, 2025

Article Review #2: Revealing the Realities of Cybercrime in Small and Medium Enterprises

Introduction

The article *"Revealing the Realities of Cybercrime in Small and Medium Enterprises: Understanding Fear and Taxonomic Perspectives"* by Arroyabe, Arranz, Fernández de Arroyabe, and Fernández de Arroyabe (2024), published in *Computers & Security*, explores how small and medium-sized enterprises (SMEs) experience and perceive cybercrime. Using Cyberspace Theory as a theoretical perspective, the authors analyze the motives and effects of cyber incidents and how fear shapes SMEs' cybersecurity behavior. Drawing data from over 12,000 SMEs across Europe, the article emphasizes that cybersecurity challenges extend beyond technology, reflecting deeply social, psychological, and organizational factors that determine how SMEs respond to digital threats.

Relation to Social Science Principles

This study connects strongly with the principles of the social sciences because it focuses on human behavior, organizational decision-making, and perceptions of risk. The concept of fear and perceived vulnerability is psychological, while the analysis of organizational behavior and resource inequality reflects sociological and economic dimensions. The study shows that cybersecurity is not only a technical issue but also a social one shaped by beliefs, attitudes, culture, and access to resources. By linking cyber risk perception to institutional behavior, the authors demonstrate that technological readiness depends largely on social understanding and shared norms within organizations.

Research Questions, Hypotheses, Independent and Dependent Variables

The research primarily asks: What motivates cybercrime against SMEs? How do SMEs perceive the fear of cybercrime? And how does fear influence their cybersecurity behavior?

While the study is exploratory and not based on formal hypotheses, it implies that higher levels of perceived fear are associated with stronger cybersecurity practices (Arroyabe et al., 2024). The independent variables include SME characteristics such as size, sector, location, and perceived risk, while the dependent variables include cybersecurity behavior, digital engagement, and the resulting taxonomic classification of SMEs based on fear levels.

Research Methods

The study employs a quantitative survey method, using data from the Flash Eurobarometer No. 496, which covered 12,863 SMEs across 27 European Union member states. It applies to a taxonomic approach to classify SMEs based on their cybercrime fears and behaviors. The large sample size and statistical modeling enhance the study's reliability and allow meaningful generalizations about SME behavior toward cyber risk.

Data and Analysis

The data includes SME demographic information, levels of digitalization, prior experience with cyberattacks, and perceived fears related to cyber threats. Statistical and cluster analysis techniques were used to identify relationships between variables and classify SMEs into profiles. Arroyabe et al (2024) indicates that the findings reveal that SMEs with higher exposure to digital technology and past attacks experience greater fear and are more likely to implement protective measures. Conversely, those with low digital engagement often underestimate their vulnerability, leaving them exposed to significant cyber risks.

Connection to PowerPoint Concepts

The article connects closely to class presentations on digital ethics, risk perception, and human factors in cybersecurity. It supports the idea that cybersecurity involves people and organizational culture as much as technology. The authors' discussion of fear aligns with social

science concepts of behavioral response and decision-making under uncertainty, while their emphasis on organizational behavior reflects topics on digital responsibility and ethical management.

Relations to Marginalized Groups

This topic also relates to the challenges faced by marginalized groups, as SMEs are economically vulnerable compared to large corporations. Many SMEs lack financial and technical resources to maintain strong cybersecurity defenses. This inequality mirrors broader social disparities where smaller or less resourced groups face higher exposure to risk. The article, therefore, highlights the need for inclusive cybersecurity policies that consider these structural disadvantages.

Contributions to Society

The study makes a significant contribution to society by promoting awareness of how social, emotional, and organizational factors shape cybersecurity behavior. It encourages policymakers and business leaders to design training, awareness, and support programs for SMEs, ensuring digital safety is accessible to all. The research also contributes to academic understanding of how fear and perception influence technological engagement, thereby promoting a human-centered approach to cybersecurity management**.**

Conclusion

In summary, the authors demonstrate that cybersecurity is not merely about technology; it is about people, perceptions, and social systems. By exploring how SMEs experience and respond to fear, the study bridges the gap between social science and cybersecurity research. Its insights remind society that achieving digital safety requires addressing human behavior and resource inequality alongside technical solutions.

Reference

Arroyabe, M. F., Arranz, C. F. A., Fernández de Arroyabe, I., & Fernández de Arroyabe, J. C. (2024). Revealing the realities of cybercrime in small and medium enterprises: Understanding fear and taxonomic perspectives. *Computers & Security, 141,* 103826. https://doi.org/10.1016/j.cose.2024.103826