Celeste Meraz-Luna

Diwakar Yalpi

CYSE 201S

April 6, 2025

Article Review #2 An Empirical Study of Ransomware Attacks on Organizations

Ransomware attacks have become one of the most critical threats facing organizations in the digital age. The article "An Empirical Study of Ransomware Attacks on Organizations" by Connolly et al. (2020) explores the severity of ransomware attacks and the factors influencing organizational vulnerability. This review will examine how the article relates to the principles of the social sciences, the research methods used, and its contributions to the field, particularly regarding marginalized groups and broader societal implications.

Principle of Social Sciences Related to the Article

The study of ransomware attacks ties into various principles of the social sciences, particularly in understanding human behavior, organizational dynamics, and societal implications. One of the social science examples is behavioral economics, it is the study of how individuals and organizations assess risk in cybersecruity and how it aligns with the behavioral economics principles. A second example is the sociology of organizations, and how organizations response to ransomware attacks reflects sociological theories about how institutions adapt to crisis and how internal factors shape responses to cyber threats. A third example is the political science reflecting on the broader political implications of ransomware attacks on national security and the economy are significant.

Study's Research Hypothesis

The authors were able to explore several key questions related to ransomware attacks. The central research questions include “What are the factors that influence an organization’s vulnerability to ransomware attacks?” and “How do organizations assess the severity of the attack and decide whether to pay the ransomware?” The hypothesis addressed the relationships between organizational characteristics and the severity of ransomware attacks, with the expectation that more prepared organizations would experience less severe consequences.

Types of Research Methods Used

The authors employed a mixed methods approach. They conducted a quantitative analysis of ransomware attack incidents, utilizing a dataset from multiple organizations across different industries. Qualitative data was gathered through interviews with cybersecurity professionals to better understand the experiences and responses of organizations facing such attacks. This approach allowed for a comprehensive analysis of both the frequency and severity of attacks and the organizational factors influencing vulnerability.

Types of Data and Analysis Done

The data included incident reports, cybersecurity audits, and interviews with organizations leaders and IT professionals. The quantitative data was analyzed to identify patterns in attack frequency, the size of affected organizations, and the security measures in place before the attack. The qualitative analysis involved thematic coding to identify common themes in organizational responses, such as decision-making processes regarding ransomware payment and long-term recovery strategies.

Article Relates to Class Topics

Several concepts discussed in the class topics, especially in relations to cybersecurity risk management, are reflected in the article. The concept of cybersecurity preparedness relates to how organizations that are better prepared tend to experience less severe impacts from ransomware attacks. Additionally, the cost-benefit analysis of paying ransomware versus recovering from the attack without payment aligns with economic theories presented in the course, emphasizing the trade-offs organizations must consider when confronted with cybercrime.

Challenges, Concerns and Contributions of Marginalized Groups

Ransomware attacks disproportionately affect marginalized groups in several ways like the disproportionate impact on smaller businesses. Many smaller organizations, which are often owned by marginalized communities, lack the resources for robust cybersecurity defenses. These businesses are more vulnerable to ransomware attacks and are less likely to recover quickly without significant financial or social support. Another way ransomware can affect marginalized groups is in the access of cybersecurity resources. Marginalized groups, particularly in low-income or developing areas, often lack access to the latest cybersecurity training, software, and infrastructure. This creates a significant vulnerability, as these groups may not have the knowledge or tools to defend against ransomware attacks effectively.

Contributions of the Studies to Society

The article makes important contributions to both the cybersecurity field and broader societal understanding of ransomware threats. By identifying key factors that influence organizational vulnerability, the study provides actionable insights for organizations looking to strengthen their defenses against ransomware. This can help businesses reduce the severity of

attacks and better allocate resources for cybersecurity. Also, the study contributes to the ongoing conversation about the regulation of cybersecurity and the need for governmental oversight in protecting organizations from cybercrime. Policymakers can use the finding to craft more effective strategies for mitigating ransomware risks and supporting affected organizations.

Conclusion

Connolly et al.'s (2020) study on ransomware attacks provides valuable insights into the severity of cyber threats and the factors influencing organizational vulnerability. By drawing connections between organizational preparedness, cybersecurity practices, and the broader social implications of these attacks, the authors offer crucial recommendations for both businesses and policymakers. The study also highlights the unique challenges faced by marginalized groups, emphasizing the need for more equitable access to cybersecruity resources. Ultimately, the research contributes to society by offering guidance on improving organizational defenses and informing policy decisions that can reduce the risk associated with ransomware.

References

Lena Yuryna Connolly, David S Wall, Michael Lang, Bruce Oddson, An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa023, https://doi.org/10.1093/cybsec/tyaa023