Article Review 2

An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability

Stephen Price

School of Cybersecurity, Old Dominion University

CYSE201S: Cybersecurity and Social Science

Professor Diwakar Yalpi

November 16, 2025

Introduction

Ransomware has remained one of the most dominant threats for public and private entities not only within the UK and North America, but around the world outside-Europe. Ransomware is a type of malware where attackers encrypt people's files making them unable to access it and demands a ransom or payment in order for people to regain their access back. Since ransomware started in 2013 it has evolved overtime. It-has network defenders that have made important advances like sophisticated detection methods and innovative prevention that can help organization implement policies, technical controls, and proper security measures so they won't fall victim to ransomware attacks.

Research Question and Hypotheses

The main research question in this study is What factors like organizational size, sector, and security posture influence the degree of severity experienced by an organization following a ransomware attack? The hypothesis of this study is that an organization's size affects the severity of a ransomware attack. The independent variables for this study are the organizational size, attack type, organization security posture, and the organization sector. The dependent variable for this study is the degree of severity of the ransomware attack.

Research Methods

The research methods that were used in this study are both quantitative and qualitative for data collection and analysis. Quantitative data was assessed by collecting 55 ransomware attacks across 50 organizations from the UK and North America. An impact assessment exercise was done for statistical testing of the hypothesis. This research collected data on organization's profiles and characteristics of the attacks. A qualitative method was performed through

interviews where people from victim organizations provided information about their experiences to help build the quantitative variables.

Data and Analysis

This study collected and analyzed mostly quantitative data through statistical tests, descriptive statistics, and a qualitative interview. The statistical test analyzed two variables the posture and the attack severity. Descriptive statistics were used to compare the percentages of public and private organizations to look at the severity of ransomware attacks across different independent variable categories. A qualitative interview was done to help researchers categorize the key variables like the security posture for the quantitative research.

Social Science Concepts

This article can relate to the conflict theory where there are power differences and inequality in our society. In the article this occurs with the public and private sector organizations where private sector organizations have experienced more severe attacks than public sector organizations. This can be viewed as conflict because different types of organizations possess different motivations and resources that can affect their ability to defend or recover from ransomware attacks.

Marginalized Groups

This article doesn't really focus on marginalized groups too much, but it has suggestions for marginalized groups that concern issues like resource disparity and access to protection. The article confirms that weak security can lead to ransomware attacks being more severe. Small organizations may have weak security due to financial constraints. Small and Mid-sized Enterprises (SMEs) most of the time represent more vulnerable organizations that is run by or

employing marginalized groups. High severity across all organization sizes can suggest that resource limited SMEs cannot afford strong security are disproportionately exposed causing instability for lower income employees.

Society Contributions

This article can contribute to society by informing policies that ransomware is not only a technical problem but an organizational business problem also. The article shows that an organization's sector and security posture are the main factors of the severity of a ransomware attack. This can be used to inform policymakers and organization owners that resources should be used toward improving the organization's security posture and human security awareness to minimize the likelihood or possibly prevent from being vulnerable to ransomware attacks.

Conclusion

In conclusion, the hypothesis was incorrect the article showed that organizations can control their own destiny on how vulnerable they are to ransomware attacks. An organization's internal controls, policies, and management is more important than the organization size. This can help strengthen organizations by focusing on investments like employee training, organization governance, and security culture rather than ONLY buying and using technical tools that can help improve the organization security posture and be able to detect, defend, or protect themselves from ransomware attacks.

References

Connolly, L. Y., Wall, D.S., Lang, M., & Oddson, B. (2020). An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, 6(1), tyaa023. empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability | Journal of Cybersecurity | Oxford Academic