A Study in Ransomware Severity and the Effect on Organizations

Article Review #1

Samantha Riggs

10/1/2024

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

Relation to the Principles of Social Science:

The study reviewed discusses a study in vulnerability, specifically concerning ransomware that affects organizations. The article itself states that this was an empirical study of these topics, which indicates that this study was completed without relying on assumptions or personal opinions. Performing a study while applying this principle of social sciences allows for the reduction of any potential bias or false information being taken into account due to simple assumptions.

Secondly the principle of ethical neutrality was applied to this study. It was approved by the Ethics Committee at the University of Leeds, and "all necessary precautions were followed to ensure the anonymity of study participants and the confidentiality of collected data." (Connolly, *et.al* 2020). By adhering to ethical standards, it provides confidence that the study is unbiased, and by extension, add a level of credibility to the study.

Additionally, the principle of objectivity is thoroughly applied to this study. It is often mentioned that all findings were observed directly from the data collected, rather than stating assumptions without relating said assumptions to the data gathered. This is indicated by phrases such as "we observed" and "our findings show".

Hypotheses:

Six hypotheses were presented in this article, all of which focused on determining how different variables affected an attack's severity. There were three hypotheses based on factors concerning an organization itself , and three more concerning the different factors of an attack. These hypotheses were as follows (Connolly, *et.al* 2020):

Hypothesis 1a: An organization's size influences the impact severity of a ransomware attack.

Hypothesis 1b: An organization's sector influences the impact severity of a ransomware attack.

Hypothesis 1c: An organization's security posture influences the impact severity of a ransomware attack.

Hypothesis 2a: The crypto-ransomware propagation class influences the impact severity of a ransomware attack.

Hypothesis 2b: The attack type, i.e. opportunistic or targeted, influences the impact severity of a ransomware attack.

Hypothesis 2c: The attack target, i.e. human or machine, influences the impact severity of a ransomware attack.

Research Methods, Data Types, and Overall Analysis:

This study uses multiple research methods that follow "an exploratory sequential design." (Connolly, *et.al* 2020). The study was broken up into two phases. The first phase was meant to establish an Impact Assessment Instrument based on qualitative data that could effectively evaluate the severity of attacks, while in the second phase, more quantitative data was collected to allow for the statistical testing of all hypotheses.

In phase one, data was collected using a purposeful approach. Ten interviews were performed with professionals who work for organization's that were previous victims of ransomware specific attacks. Data concerning fifteen incidences was collected, (some of the organization's were attacked more than once). Five categories of described negative outcomes

were formed from the data. The data under each category allow impact descriptors to be developed, (low, medium, and high).

Data collection for phase two was performed by performing interviewing with police officers that had previous experience dealing with ransomware attacks. The study notes this was done opposed to interviewing organizations due to how much time it took to find organizations that would share such sensitive information. The questions asked and information gathered was also more quantitative in nature when compared to phase one.

A number of conclusions were made from the information gathered and analyzed in this study. 1. The size of the organization, in terms of ransomware, does not affect the severity of these attacks. 2. Ransomware attacks are indiscriminate, and the severity is not influenced by whether the target is focused on human vulnerability or machine vulnerability. 3. Organizations in the private sector are more likely to have more severe effects from the attack. 4. A relationship between an organization's security posture and the severity of an attack was supported by this study.

Class Concept Relation:

One large concept from the class presented so far that can be applied is the Routine Activity Theory presented in Module 5. This article makes the point that vulnerabilities present in an organization's systems should be addressed because offenders are aware of the dependency the organization has on the system as well as the data contained within it. This aligns with this theory as there is 1. A potential offender; 2. A suitable target, which in this case is an

organization with sensitive data; and 3. The absence of effective security measures and the existence of potential vulnerabilities.

Different principles of social science were applied to this study, (as discussed previously), all of which were discussed within Module 1. These were the empirical principle, the principle of ethical neutrality, and the principle of objectivity.

Surveys and interviews were the main method of data collection within this study, connecting with Module 3, which discussed the various strategies to study cybersecurity through an interdisciplinary lens. Also discussed in Module 3, archival research was conducted in this study, as prior literature was referenced multiple times as resources in the article.

Societal Impact:

This study states that a gap is present in terms of literature relating to the examination of ransomware from both a company's and its user base's perspective. The article states that the study "aims to make a contribution towards addressing this gap." (Connolly, *et. al* 2020). By increasing the knowledge and literature present as resources, better strategies can be developed and implemented within systems, which not only aids the general population, can be adapted to fit organizations such as non-profits and social services that serve marginalized communities.

An additional impact of this study would be providing strategies for smaller businesses and other community organizations. As the study stated, the size of the organization holds no statistically significant impact on attack severity, indicating that the same methods used for companies and organizations that have a large number of profits and data at stake can be used to provide recommendations to these smaller, community-based businesses. Furthermore, these

strategies and recommendations would allow these businesses to recover quicker from an attack, should one happen and be successful.

Conclusion:

Throughout this review of an empirical study of ransomware and the severity of such attacks, multiple different topics were discussed. The hypotheses, research methods, as well as the types of data and analysis performed was discussed. Additionally, comparisons and connections were made from this article to in-class concepts. Furthermore, the potential societal impact on the general population and marginalized communities from this study was discussed.

References:

Connolly L., et. al (2020, December). *An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability.* Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/6/1/tyaa023/6047253?searchresult=1