Diane Gilzow

April 10, 2025

CYSE 201S

The Effects of Ransomware on Organizations

The article that I reviewed was published in the Journal of Cybersecurity by Oxford Academic that explored the impact of ransomware attacks on organizations. It addressed how severe ransomware attacks can be on an organization and explained key factors that can influence the severity of an attack.

Research Question and Hypothesis

The main question the article poses was how severe the effects of ransomware attacks are on organizations. It specifically explores whether an organization's size and what sector it's in will influence the severity of a ransomware attack. It also questions if an organization's security practices will also influence the severity of a ransomware attack.

Research Methods

The study mainly utilizes qualitative methods to measure the severity of ransomware attacks on organizations. Interviews were conducted with a sample of random organizations that had experienced ransomware incidents, asking them to rate the severity of the attacks on a scale of low, medium, or high.

Data and Analysis

Based on the data that was gathered, it was found that the organizational size did not indicate the severity of a ransomware attack, where both small and medium-sized enterprises (SMEs) and large organizations have faced high severity ransomware attacks. However, whether an organization was part of the private or public sector did play a role in determining the severity of ransomware attacks, where private organizations were more likely to face ransomware attacks of high severity than public organizations. Additionally, organizations with weaker security posture were more likely to experience much more severe ransomware attacks than organizations with medium or strong security postures, where 80% of organizations with a weak security posture have been hit with severe ransomware attacks.

Social Science Principles

Four social science principles that correlate with the article are objectivity, parsimony, skepticism, and determinism. The article uses objectivity to consider every point of view when it comes to how ransomware affects organizations. Determinism was also addressed by exploring how specific human behaviors, such as poor cyber hygiene or weak security practices, determines how an organization gets a ransomware attack. Parsimony is used to present complex terms in simple detail, such as the definition of security posture. Skepticism is also applied in the article as it considers multiple factors and explanations of ransomware attacks on organizations.

Concepts from Class that Relates to the Article

One concept that the article emphasizes is how human error often contributes to the increased risk of a ransomware attack. It was found in the study that having a weak cybersecurity

posture within an organization can contribute to an increased risk of a ransomware attack, which ties in to the importance of maintaining proper cybersecurity culture and hygiene within an organization. While on the topic of human error, the article mentions that humans are often targeted through the means of social engineering tactics, rather than targeting "machines" which may be exploited by a vulnerability. Economics also come into play in this study; private organizations were found to face more severe ransomware attacks since most of their business model revolves around generating profit. Therefore, when a private organization is faced with a ransomware attack, the consequences are much more severe than that of a public one.

Marginalized Groups

A common group that can be often targeted by ransomware attacks are people or organizations that have a small budget or do not have an economic advantage. The stress caused by a ransomware attack can be distressing, especially for business owners, and may lead to mental health concerns. Another marginalized group that are often targeted by ransomware attacks are healthcare organizations, since they typically have limited cybersecurity resources and valuable data that is sought out. If a healthcare system goes down, it can affect patients and put their lives at risk.

Contributions to Society

The hypothesis the article poses are meant to help address what kind of organiztions are more susceptible to ransomware attacks. It points out common factors that organizations may share when they face a ransomware attack with severe consequences, which is frequently due to having weak security postures that need to be improved on. It also makes a point that

ransomware consequences will cost a lot financially, whether the ransom is paid off or if money is going to go towards recovery. Therefore, organizations will need to invest in cybersecurity resources rather than face the p consequences of a ransomware attack.

Conclusion

The article brings awareness that any organization, no matter the size, can be a victim to a ransomware attack. Ransomware has become one of the most prevalent and disruptive cybersecurity threats that bring harm to many businesses. The study conducted in this article addresses how being in the private or public sector and the quality of security practices influence the severity of a ransomware attack. It was found that organizations in the private sector and weak security practices would influence more severe ransomware attacks. The study ultimately brings out the importance of implementing cybersecurity measures into an organization to mitigate the impact of ransomware attacks.

References

Empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability | journal of cybersecurity | oxford academic. (n.d.). https://academic.oup.com/cybersecurity/article/6/1/tyaa023/6047253