Ennio Cruz

Professor Duvall

CYSE201s

4 NOV 2023

Article Review 2:

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

https://doi.org/10.1093/cybsec/tyaa023

The article I chose to review is a study that analyzes crypto-ransomware attacks, how they affect organizations, both public and private, and the possible factors that determine the severity of their effects. The article has several hypotheses but can be narrowed to two main questions. First, regarding the organization, “Do factors such as size, sector, and security posture of the organization affect the severity of crypto-ransomware attacks?” and the second, regarding the crypto-ransomware, “Do factors such as propagation class, attack type, and attack target affect the severity of crypto-ransomware attacks?”

The researchers had to create an impact assessment tool to tabulate the severity of crypto-ransomware attacks. The impact assessment tool created defined the following factors as follows:

Organization Factors:

- Size – refers to small/medium enterprise or large enterprise.
- Sector – refers to public organizations or private organizations.
- Security posture – refers to weak, medium, or strong security posture.

Crypto-ransomware Factors:

- Propagation attack – refers to the type of crypto-ransomware used by either Gen II or Gen III.
- Attack type – refers to either a targeted or opportunistic attack.
- Attack target – refers to a human or machine target.

To test the hypothesis, the researchers used a multi-method approach that included interviewing cybersecurity experts and studying archival data on ransomware attacks. The researchers interviewed 10 IT/Cybersecurity experts who were part of different-sized organizations, both public and private, that suffered a crypto-ransomware attack. They also interviewed 10 law enforcement officers with cybersecurity expertise who handled crypto-ransomware cases. The interview questions included asking for details regarding the severity of the crypto-ransomware attack, such as the following:

- How long were business functions disrupted?
- How much information was lost?
- How critical to business was the encrypted information?
- What are the affected devices?
- How long was the recovery time?

The researchers also analyzed crypto-ransomware incident reports from 50 organizations from varying factors of size, sector, and security posture. Recording the severity of the crypto-ransomware attacks described in the incident reports based on the same interview questions while recording factors such as propagation attack, attack type, and attack target.

The researchers tabulated the data gathered from the interviews and archival research into their impact assessment tool, which resulted in the following conclusions:

Organization Factors:

- Size – non-factor.
- Sector – private organizations are more severely impacted.
- Security posture – weak security posture is more severely impacted.

Crypto-ransomware Factors:

- Propagation attack – non-factor.
- Attack type – Targeted attacks are more severe.
- Attack target – non-factor.

Based on their data analysis, the researchers have concluded that size plays no factor in severity because both small/medium and large organizations are equally susceptible to severe ransomware attacks. Crypto-ransomware attacks are more severe in private organizations because their customers can permanently leave, making them unable to sustain profit, unlike public organizations that are often state-owned and are sole service providers. Crypto-ransomware attacks are severe when the security posture is weak, regardless of organization size and sector. Propagation attacks play no factor because even older generations of ransomware can have a severe impact on organizations with weak security. Targeted crypto-ransomware attacks are more severe because the exploitation is planned to maximize disruption that would warrant high ransoms devastating to organizations. Both human and machine attack factors are concluded as non-factors because the severity of both is more determined by weak overall security posture.

These conclusions can be related to the principle of determinism, such as the presence of a factor such as weak security posture certainly determines the outcome of severe impact. It is also parsimonious and laid out simply how the factors may or may not have any effect with severity at all. The data gathered and used are also empirical, which relates to the principle of empiricism.

The article could also be related to several concepts discussed in class. The article is a great example of the interdisciplinary nature of cybersecurity and how sociology influences it. The conclusions of the article mentioned social factors such as the sector of the organization, consumers react differently to public and private organizations that suffer crypto-ransomware attacks, and consumers can permanently leave private organizations, which causes them to be more impacted severely.

The article also stated that targeted attacks are more severe, this can be related to class discussions regarding social engineering. Crypto-ransomware attacks that utilized social engineering severely impacted its target organization because they effectively exploited vulnerabilities and were able to encrypt most of the organization's data.

The article also briefly details the concept of human factors. Human error in cybersecurity practices, regardless of the size and type of organization, leads to weak security posture, which influences the severity of crypto-ransomware attacks, and human factor programs such as cyber awareness training are important.

In class, we discussed how cybersecurity cultures in organizations are important in maintaining a strong security posture. The article details findings that private organizations with weak security posture were often due to cost-benefit analysis and choosing profit over mitigating risk. It displayed an organizational culture that did not value cybersecurity and resulted in the severe impact of crypto-ransomware attacks because the organization was not prepared to respond to them.

In relation to the cybersecurity concerns of marginalized groups, the article focuses on the severity of crypto-ransomware attacks on different organizations. The two main concerns are privacy breaches and consumer trust among vulnerable populations. An example would be minority populations that rely on smaller local banking institutions. Although the size of the organization does not matter and both small/medium and large organizations can equally suffer severe impact from crypto-ransomware, larger organizations have a higher chance of recovering from severe impact than smaller organizations, possibly leaving marginalized groups disproportionately impacted if a local bank is forced to close.

The article also provides important contributions to the current body of studies. It identifies factors that increase the severity of crypto-ransomware attacks that can be used by organizations to identify their own weakness and what they can improve. It also provides a robust impact assessment tool that other researchers can refer to in conducting further studies.