Summary:

Ransomware is a significant cybersecurity threat, causing data breaches and disruptions. However, many studies lack consideration of government strategies, industry guidelines, and cyber intelligence. A study evaluating 212 academic studies found that many were irrelevant to the current reality. The study proposed prioritizing data exfiltration over encryption, considering ransomware in a business-practical manner, and recommending collaboration with the industry to address this evolving threat.

This survey compiled the ransomware evolution history and applied Rogers' Innovation Adoption Curve, predicting the rise of destructive ransomware with espionage. It reviewed 212 academic studies and found that most research has become less relevant in the era of ransomware double extortion with data exfiltration. The survey proposed integrating ransomware risk management into organizational cybersecurity risk management, emphasizing government strategies, industry reports, guidelines, and cyber intelligence. It also discussed innovative research prospects, including generative AI, and suggested future research directions.

[Paper link:](https://dl.acm.org/doi/10.1145/3691340)