# Article Review #1: Valuation of Confidentiality and Availability in a Personal Ransomware Attack Scenario

**Jamil P, September 30, 2025**

## Introduction

This study focuses its view on the economic and psychological considerations of individuals by assessing their willingness to pay under controlled scenarios. The authors have employed particular methods, derived from behavioral practices, to quantify the economic value of intangible goods, such as data availability and confidentiality (Gassmann et al., 2025). This experiment pries into cognitive biases and emotional drivers, incorporating psychological constructs such as risk and perception. Finally, by framing data breaches as crime events, this paper can delve into criminological theory via offender behavior, deterrence, and victim decision-making.

## Research Question, Hypotheses, IV, and DV

The pursuit of the authors starts with the question: What do individuals value more on their private computers, availability or confidentiality of data? Such a question's answer can be found with the guidance of two hypotheses. First, more people, when under threat of data availability, will comply as opposed to confidentiality. Second, the payment amounts made will be higher under the threat of data availability versus compromised confidentiality (Gassmann et al., 2025). The independent variable is the type of threat, either the availability of data or confidentiality. The dependent variables are whether the person decides to pay and how much they pay.

# Article Review #1: Valuation of Confidentiality and Availability in a Personal Ransomware Attack Scenario

## Research Methods

The authors conducted this experiment with a between-subjects online survey whose qualified participants included 857 Germans (Gassmann et al., 2025). Half of the participants were recruited via Clickworker, a crowdsourcing platform, and were given compensation. The other half were uncompensated university participants. All were given the question pertaining to how they stored their files and their backup habits. Then, a random assignment of one of two ransomware scenarios: loss of encrypted data or loss of unencrypted data. Presented with a mock ransom note with calls for urgency of payment. Immediately after scenario exposure, comprehension quizzes and attention checks were issued to determine data quality. Following this, emotional responses were measured via the PANAS scale (Watson, Clark, & Tellegen, 1988). Finally, details regarding demographic, digital-behavioral, and economic perspectives were collected.

## Data Types and Analyses

Data types used in this experiment are categorical and continuous. Categorial types included scenario condition, payment decision, and demographics. Continuous types were payment amounts, age, and PANAS factor scores. The analysis consisted of descriptive statistics such as percentages paying, medians of those who didn't pay. Logistic regression to identify predictors of paying against not paying. Finally, linear regression to find drivers for people who paid, looking only at payments above zero and adjusting the numbers to make patterns clearer. Also grouping the 20 PANAS emotions into four main types: afraid, enthusiastic, interested, and hostile (Watson et al., 1988).

# Article Review #1: Valuation of Confidentiality and Availability in a Personal Ransomware Attack Scenario

## Integration of PowerPoint Concepts

Several concepts from the PowerPoint lectures directly apply, such as the number of people willing to pay versus those who accepted the damage. Exploring how individuals' willingness to pay to protect personal data demonstrates the vitality of non-market goods and how it can be economically valued. Highlighting the context-dependent biases that show the framing of threats influence on perception. Threats of availability are treated urgently, while confidentiality threats are viewed as distant, reflecting principles from prospect theory (Kahneman & Tversky, 1979) and hyperbolic discounting (Laibson, 1997). PANAS incorporation addresses the influences of emotion on decision-making, which supports the dual-process model where intuitive and emotion-driven systems interact with rational and deliberative systems (Kahneman, 2011). Finally, the study is designed to reflect best practices for keeping survey validity and reliability. Incorporating attention checks and comprehension quizzes aligns with the standards presented in the "Research Design" module.

## Relevance to Marginalized Groups

Ransomware incidents are considerably more targeted against public institutions with strained cybersecurity than private, fully funded corporations. Although this study sample leans towards the young and tech adjacent, its insight into emotional responses and backup behaviors reveals universal behaviors and, by proxy, structural inequities. For example, lower-income individuals were more likely to refuse payment when faced with the threat of availability. Suggesting their refusals are tied to lacking both financial means and accessible support. Such awareness could be used in developing research to better address these disparities in marginalized groups, like subsidized solutions and public campaigns.

## Societal Contributions

This research can deepen our understanding of the prevalence of cybercrime and the human cost it incurs. Offering a direct comparison between the valuation of data availability and confidentiality, in most cases displaying a willingness to pay almost equally for both. Also showing that emotional states, notably fear and hostility, are significant contributors to the decisions of payment and amounts. Offering valuable insights for strategies in crisis communication used by internet companies and law enforcement. The study indicates clear factors of vulnerability, such as income level, backup quality, and awareness of cybercrimes. This can be most useful for risk-assessment models and to distribute support more effectively. Finally, it provides empirical evidence which can inform policy and regulatory efforts to readjust data-protection disclosures and structured ransomware response frameworks.

## Conclusion

The authors have presented a rigorous investigation into how individuals, when faced with ransomware threats, value their personal data economically and emotionally. With utilization from perspectives of economics, psychology, and criminology, we can see the nuanced decision-making patterns in digital personal threats. While imminent loss of data availability often motivates payment, financial constraints and emotional responses have led to resistance. Knowing that people value data availability and confidentiality nearly equally highlights how complex it is to determine data worth. Methodologically, the study is practical for its iterative scenario testing, ensuring results validity through comprehensive variable collection and robust regression analyses. Producing a high standard that social-science research can draw on for cyber victimization. Allowing the enhancement of social work to broaden with demographic representation and examine strategies that promote effective backup behaviors and ethical resistance to criminal coercion.

## References

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. Crime and Justice, 6, 147–185.

Gassmann, F., Beck, J., Gourmelon, N., & Benenson, Z. (2025). Valuation of confidentiality and availability in a personal ransomware attack scenario. Journal of Cybersecurity, 11(1), tyaf022. https://doi.org/10.1093/cybsec/tyaf022

Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. Econometrica, 47(2), 263–291.

Laibson, D. (1997). Golden eggs and hyperbolic discounting. The Quarterly Journal of Economics, 112(2), 443–478.

# Article Review #1: Valuation of Confidentiality and Availability in a Personal Ransomware Attack Scenario

Watson, D., Clark, L. A., & Tellegen, A. (1988). Development and validation of brief measures of positive and negative affect: The PANAS scales. Journal of Personality and Social Psychology, 54(6), 1063–1070.