# Ransomware Economics: A Two-Step Approach To Model Ransom Paid

Tom Meurs*, Edward Cartwright†, Anna Cartwright‡, Marianne Junger*,
Raphael Hoheisel*, Erik Tews * and Abhishta Abhishta *
* University of Twente, Enschede, The Netherlands
Email: t.w.a.meurs@utwente.nl, m.junger@utwente.nl
r.e.hoheisel@utwente.nl, e.tews@utwente.nl
s.abhishta@utwente.nl
† De Montfort University, Leicester, Leicestershire, United Kingdom
Email: edward.cartwright@dmu.ac.uk
‡ Oxford Brookes University, Oxford, Oxfordshire, United Kingdom
Email: a.cartwright@brookes.ac.uk

***Abstract*—Ransomware poses a significant and pressing challenge in today's society. Mitigation efforts aim to reduce the profitability of ransomware attacks. Nevertheless, limited research has analysed factors that influence the size of ransom and willingness of businesses to pay a ransom. This study aims to address this existing gap by conducting an empirical investigation that focuses on the ransom paid by victims. Extending on past research, we analyse 382 ransomware attacks reported to the Dutch Police and/or handled by an Incident Response (IR) company. One challenge of modeling ransom payments is the large proportion of victims who did not pay, which leads to zero-inflation. We tackled this problem by employing a hurdle model, which effectively deals with zero-inflation by capturing ransom paid as a two-step decision-making process: first, victims decide whether to comply with the ransom demands, and if they choose to do so, they then need to determine the acceptable ransom amount. The results indicate that the presence of backups and the decision to go to an IR company play a pivotal role in the decision whether to pay the ransom or not. In addition, our findings identify insurance coverage, data exfiltration, and annual revenue of the victim as key determinants affecting the ransom amounts. Specifically, having insurance results in ransoms that are 2.8 times larger, data exfiltration corresponds to a 5.5 times increase in the ransom, and each 1% increase in a victim's yearly revenue causes a 0.12% rise in the ransom paid. In concluding our paper, we present practical policy recommendations that take into account the two crucial decision-making steps outlined in our study, focusing on data exfiltration and insurance.**

***Index Terms*—ransomware, ransom paid, insurance, backups, data exfiltration, profitability, cybercrime, willingness-to-pay, hurdle model**

## I. Introduction

Over the past few years, crypto-ransomware has emerged as a major concern for society, as reflected in Europol's consistent recognition of crypto-ransomware as a top priority [15], [16]. In the United States alone, [4] estimates that 576 organizations fell victim to crypto-ransomware attacks in 2021 with 159.4 billion USD in downtime costs. Crypto-ransomware, ransomware for short, is a type of malware that encrypts files, allows victims to regain access upon paying a ransom to the attackers. The surge in ransomware attacks can be attributed to its profitability [7], [11]. Furthermore, [21] highlights that criminals are incentivized to target victims who highly value their data, leading to increased social welfare costs. To address the surge in ransomware attacks and mitigate the impact, efforts must be made to reduce the profitability of ransomware attacks.

To reduce ransomware profitability, [17] proposes three defensive strategies: lowering the value of ransom payments, increasing the costs of ransomware attacks, and decreasing the willingness of victims to pay. The present study focuses on the profitability of ransomware attacks by focusing on the victims' decision-making to pay a certain ransom amount.

Criminals profit from ransomware attacks primarily because victims choose to pay the ransom [6], [19]. Various sources provide insights into the size of ransomware payments in recent years. An empirical study of ransomware attacks reported to the Dutch Police from 2019 to 2022 indicated an average ransom demand of 720,256 euros, with 21% of victims actually paying the ransom, resulting in financial losses of 433,191 euros [25], as victims have estimated when they reported to the police.

A company tracking ransomware payments on the Bitcoin blockchain, estimated the total ransomware payments to be 765 Million USD in 2020, 766 Million USD in 2021, and 457 Million USD in 2022 [10]. They attribute the drop in ransomware revenue in 2022 not to fewer attacks but to victims' reduced willingness to pay ransomware attackers. Interestingly, more than 50% of the revenue is concentrated among the top 5-7 strains, while the total number of strains is estimated to be around 10,000 [10].

[31] constructed a data set using ransom notes uploaded by victims, which indicated a cumulative ransom payment of 101,297,569 USD between 2017 and 2022. Additionally, [37] monitored 41,424 victims from 2012 to 2021, revealing a combined ransom payment of 176 Million USD.

Combined, these figures provide an approximation of the profitability of ransomware attacks. However, it is crucial to highlight that the social welfare costs are significantly higher, as the ransom paid merely represents a fraction of the victims'

recovery costs [4], [6], [25] and there are non-monetary costs like psychological costs, social costs and impact on customers and service users [32].

A complimentary way for criminals to profit from ransomware attacks emerges through data exfiltration. Present-day ransomware attacks frequently involves stealing data to pressure victims into paying, with threats of public exposure on leak pages [25], [27]. Additionally, criminals may choose to sell the stolen data to rival business competitors or other malicious actors for potential use in subsequent attacks [23], [28].

It is important to understand victims' willingness to pay to decrease ransomware attacks' profitability. A survey by [21] estimated a willingness to pay around 150 British pounds among 149 individuals in the UK. However, this study's limitations are twofold: it focused on individuals, disregarding potential differences with businesses' decision-making, and the survey lacked real-life applicability as it asked participants to speculate on hypothetical scenarios rather than reporting real-life situations. In a follow-up study, [8] found that a proportion of individuals appear to reject paying any ransom.

An alternative approach is provided by [11]. They conducted interviews with 41 ransomware victims from SMEs, large companies, and public organizations in the UK. Among them, 8 victims (20%) opted to pay, mainly to avoid bankruptcy. Conversely, 22 victims (67%) had no intention of paying. [11] proposes a two-step decision-making process: first, determining affordability, and second, evaluating the advantages and disadvantages of paying versus alternative data retrieval methods to minimize disruption and further financial losses.

The primary aim of this study is to apply a quantitative model to capture the decisions made by businesses. Given that many businesses do not pay the ransom we adopt a hurdle model approach to capture factors that influence payment of a ransom and factors that influence the amount of ransom paid. This statistical approach can be seen to capture the two-step decision making process proposed by [11]. We state the main research question as follows: *What factors determine the ransom paid during ransomware attacks?* To answer this question, we focus on three sub-questions:

**RQ 1:** Which factors determine whether victims will pay or will not pay the ransom?

**RQ 2:** In case the victims decide to pay, which factors determine the ransom amount victims will pay?

**RQ 3:** Do different factors influence the ransom payment decision and the amount ransom paid?

We analyse 382 ransomware attacks reported to the Dutch Police between 1 January 2019 and 1 January 2023 and incidents handled by an Incident Response (IR) company between 21 February 2020 and 1 January 2023. To deal with zero-inflation of ransom payments and effectively capture the two-step decision-making process regarding ransom payments of victims we employ a hurdle model. Our key contributions are:

1) Extending on [25], we annotate 525 ransomware attacks reported to the Dutch Police and 116 to an IR company, therefore controlling for possible low willingness to report to the police. For our regression analysis we analyse 382 ransomware attacks.
2) We demonstrate that modeling the ransom paid to criminals could be modeled as a two-step process: whether victims choose to pay and determining the amount of ransom paid. Furthermore, we identify distinct factors influencing the first and second step.
3) More specifically, having insurance results in ransoms that are 2.7 times larger, data exfiltration increases the ransom 4.4 times, and each 1% increase in a victim's yearly revenue causes a 0.12% rise in the ransom paid.
4) We propose a method to construct a demand curve based on empirical data of ransom payments.

The outline of this paper is as follows: In §II, we discuss existing literature concerning the profitability of ransomware attacks and state seven hypotheses to answer our research questions. Subsequently, in §III, we present our data and the methodology. Afterwards, §IV presents the results obtained from our research. To conclude, we discuss our findings and outline future work in §V and §VI, respectively.

## II. Related Work and Hypotheses

Ransomware is a financially motivated crime, with cyber-criminals seeking to maximize profit by controlling the size of the ransom [11], [19], [21]. Given the relative ease of attacking victims and the low risk of capture, the ransom amount becomes a critical variable they criminals can manipulate. Therefore we make it the focal point of our analysis [21].

The criminals' potential profit heavily relies on the willingness of victims to pay the ransom, influenced by various factors such as the importance of files to the victim, the availability of recent backups, liquid funds, relative trust in the criminals, and willingness to negotiate with them. From the criminals' perspective, their focus lies on determining the maximum amount each victim is willing to pay for file recovery, also known as the willingness to pay (WTP) [21].

Heterogeneity in businesses maximum willingness to pay a ransom, incentivizes criminals to adopt price discrimination strategies, as cited in previous works [6], [19], [21]. Price discrimination increases profits by encouraging more victims to pay, as the ransom can be lowered for those with a lower WTP while keeping higher prices for others [19], [25].

If criminals do not use price discrimination between victims, which is defined as uniform pricing, criminals impose an identical ransom amount to all victims. Uniform pricing is a characteristic of certain ransomware strains like Deadbolt [26] and old ransomware strains like CryptoLocker [6].

In contrast, second-degree and third-degree price discrimination are classic price discrimination methods. Second-degree price discrimination involves offering victims diverse package options, allowing them to pay solely for the decrypter, preventing data publication, or obtaining a comprehensive security report from the criminal, or any combination of these options [19], [21], [27]. Third-degree price discrimination directly distinguishes different victim types. Criminals using third-degree

price discrimination may analyze victims' company details, including yearly revenue from public sources or obtained insurance policy documents during the attack.

Uniform pricing, second-degree and third-degree price discrimination are all pricing methods observed in real-life ransomware attacks and lead to different types of dynamics between criminals and victims [6], [19], [25], [28]. With uniform pricing, the ransom note states the ransom amount and bitcoin address in the ransom note, though this approach is becoming less common [20], [25]. In contrast, second- and third-degree price strategies typically involve negotiation through email or TOR-chat and offering ransoms based on factors like the number of servers encrypted or the services provided by the criminal, such as data decryption, prevention of data publication, or even a security report how the criminal infected the company and which security measures to take [19], [25]. Typically, an adversary initiates the negotiation by specifying an initial ransom, and the victim has the option to counter with a request for a lower price, commonly known as a discount. The negotiation progresses with both parties engaging in reciprocal offers to reach an agreement [19].

Ransomware criminals seem successful in implementing price discrimination strategies. Empirical studies (e.g., [19], [25]) have identified factors influencing the ransom requested and the WTP in ransomware attacks, such as data exfiltration, Ransomware-as-a-Service (RaaS), blackmail, victim's yearly revenue, sector, and insurance. Notably, an overlap in these factors suggests that criminals may have effectively identified variables for which victims are willing to pay, indicating successful price discrimination strategies.

A significant subset of victims consists of those who refuse to pay the ransom, as emphasized by [7], [8], [11]. For these individuals, the WTP is effectively zero. As a result, it is reasonable to distinguish between those inclined to pay the ransom and those who are not, before modeling the ransom amount they would pay. Considering the decision to pay the ransom as such a two-step procedure can be even more valuable if distinct factors influence the first and second step. For example, having off-line backups might influence the decision to pay, but not the ransom amount if the victim wants to pay. This leads to our first hypothesis:

**Hypothesis 1:** *The factors influencing the decision to pay are different from the factors influencing the ransom amount paid.*

One of the critical decision that victims face is how to mitigate the ransomware attack, especially since most victims have little experience with ransomware attacks. This lack of expertise creates tension and uncertainty, making it more likely for victims to seek specialized guidance. Especially when the situation is critical and recovery seems difficult. Therefore, many victims might consult an Incident Response (IR) company [40]. Based on this behaviour, we hypothesize that victims who turn to IR companies are more inclined to consider making ransom payments and may also be willing to pay larger ransom amounts.

**Hypothesis 2:** *Victims' decision to go to the IR company are more inclined to consider payment (H2.1) and pay larger ransom amounts compared to victims who decided not to go to the IR company (H2.2).*

Two strategies employed by companies to reduce the impact of ransomware attacks and decrease the willingness to pay (WTP) are cyber insurance and recoverable offline-backups [17].

Companies benefit from insurance coverage during ransomware incidents in multiple ways [17], [30], [40]. Firstly, insurance providers may have experience in assessing the situation and determining whether the company can recover without paying the ransom. Secondly, if payment is necessary, insurance companies may assist in negotiating and reducing the ransom amount. Thirdly, they might compensate the ransom if paid, and finally, they facilitate the company's recovery process by for example hiring an IR company [30], [40].

Furthermore, there is ongoing debate on whether cyber insurance leads companies to reduce investments in preventive security measures, as insurance coverage may alleviate the financial consequences of an attack, resulting in moral hazard. For a more elaborate analysis on the relationship between insurance and ransomware we refer to [30], [38], [40].

It is important to note that although cyber insurance may ease the financial burden on victims, it does not address the underlying incentives for ransomware attacks. On the contrary, from the attacker's perspective, cyber insurance might actually encourage more victims to pay the ransom. This could make ransomware attacks more profitable and, unfortunately, more attractive for cybercriminals.

**Hypothesis 3:** *Victims with cyber insurance are more inclined to consider payment (H3.1) and pay larger ransom amounts compared to victims with no cyber insurance (H3.2).*

Backups represent a valuable strategy for companies to mitigate the impact of ransomware attacks [17], [25]. In the event of file encryption, backups offer a means of restoring data. However, there are three complications. Firstly, attackers actively seek out and delete backups to discourage victims from relying on them and encourage ransom payment. Secondly, difficulties may arise in the recovery process, even if backups remain unaffected by criminals. Research by [39] shows that both cloud-based and colocation backup methods may incur a larger fraction of costs compared to paying the ransom. Additionally, many companies lack awareness of the time required for backup recovery, which might result in considering ransom payment to speed up the process. Thirdly, currently most criminals encrypt and exfiltrate files, threatening publication if no payment is made, imposing costs regardless of backups [23], [27]. Nonetheless, despite these challenges, we expect that having accessible offline backups will likely lead to a reduced number of companies paying the ransom, without affecting the ransom amounts [11].

**Hypothesis 4** : *The presence of recoverable backups leads victims to be less inclined to consider payment (H4.1),*

*while not influencing the ransom amount paid, compared to victims lacking recoverable backups (H4.2).*

As mentioned previously, data exfiltration is another incentive for victims to consider paying a ransom and larger ransom amount [23], [25], [27]. Companies want to prevent undesirable outcomes linked to the publication of data and the damage it could cause to their reputation.

**Hypothesis 5:** *Data exfiltration leads to victims more inclined to consider payment (H5.1) and pay larger ransom amounts compared to victims where no data is exfiltrated (H5.2).*

Another relevant factor might be the victim's yearly revenue. The victim's yearly revenue can impact the WTP due to two reasons. Firstly, it influences their ransom payment capacity [11]. Secondly, criminals might use it for second or third-degree price discrimination as described above [6], [19], [25]. Hence, the victim's yearly revenue affects the decision to pay and the ransom amount paid.

**Hypothesis 6:** *Yearly revenue of the victim influences the decision to pay (H6.1) and the ransom paid (H6.2).*

Finally, some sources describe that the ransom revenues for criminals have increased from 2019 to 2021, but decreased in 2022 [10], [25]. There are claims that insurers and businesses are reacting to the increased attacks in 2020 and 2021 and so we might expect ransoms to be falling [12]. Consequently, the final hypothesis of this study is:

**Hypothesis 7:** *The frequency of ransom paid is not different over the years (H7.1), but the amount ransom paid is (H7.2).*

## III. Data and Methodology

A strength of this study is that we use two data sets. The first is an extension of data set and methodology previously used by [25] and consists of 525 ransomware attacks reported to the Dutch Police between 1 January 2019 and 1 January 2023. The second data set are 116 incidents reported by an incident response company (IR company) active in the Netherlands between 20 February 2020 and 1 January 2023. Using another source of data in addition to police reports could help account for situations where people may be less willing to report to the police [34], [36].

To compile the Dutch Police data set, a search was conducted in the police systems employing the keyword *'ransomware'*, which was further analyzed with the authors manually classifying the incidents involving crypto-ransomware attacks. On the other hand, the incidents recorded by the IR company were specifically disclosed to the members of the team for the purpose of our project.

From both data sets we exclude attempted ransomware attacks and attacks reported by individuals, resulting in 418 ransomware attacks in the data set of the Dutch Police and 97 ransomware attacks in the IR company data set. Removing duplicates between data sets, we have a combined data set of 481 unique successful ransomware attacks on companies, see Table I.

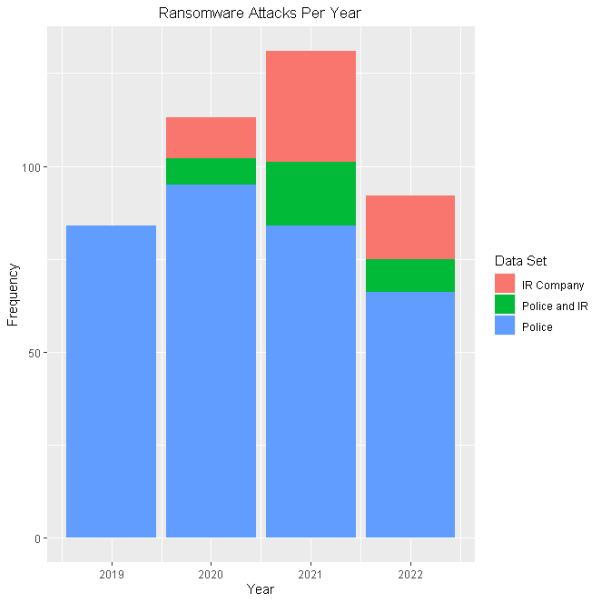


Fig. 1. Ransomware attacks per year reported to the Police, to the IR company or to both.

The Dutch Police data set is limited to cases within the Netherlands due to jurisdictional limitations. In contrast, the IR company data set comprises cases from various countries where the company was actively involved. Among the 97 attacks in the IR company data set, 42 were recorded outside the Netherlands. Given the geographical proximity of these countries to the Netherlands, it was deemed reasonable to include them in the study, as we anticipate no systematic differences from the other cases in the IR company data set.

Given the presence of both data sets, we have the opportunity to examine the willingness of victims to report ransomware attacks to the police. Within the 97 IR company cases, three distinct categories emerge: 1) 21 cases (22%) did not report to the police, 2) 34 cases (35%) reported the incident to the police, and 3) 42 cases (43%) occurred in foreign countries, and their reporting status to local authorities remains unknown. Consequently, when focusing solely on cases within the Netherlands, 34 out of 55 victims (62%) reported the ransomware attacks to the Dutch Police. A visual representation of these data sets is presented in Figure 1. There seems to be an increase of ransomware attacks in 2020 and 2021 compared to 2019 and 2020. Note that the rise in ransomware attacks in the IR company data set might be due to extra incidents in foreign countries.

Next, we describe the variables coded in this study. The **dependent variables** in our study (see Table I) are:

**1. Ransom Paid:** This section examines variables which help construct the outcome variable *1c. Ransom paid*, which is the main focus of our study.

**1a.** *Ransom requested end of negotiations:* This variable represents the final offer made by the criminal during negotiations and was measured in euros. It was used to construct *1c. Ransom paid*.

TABLE I
VARIABLES USED IN THIS STUDY AND PERCENTAGE MISSING VALUES.

| Variables | Unit / categories | Missing Values (%) |
|---|---|---|
| 1a. Ransom requested end negotiations | Euro, Log 10 transformed | 228/481 (47%) |
| 1b. Payment | Yes = 1 / No = 0 | 33/481 (7%) |
| 1c. Ransom paid | Euro, Log 10 transformed | 61/481 (13%) |
| 2a. Time negotiating | Hours | 70/481 (15%) |
| 2b. Insurance | Yes = 1 / No = 0 | 50/481 (10%) |
| 2c. Backups | No = 0, Yes + no recovery = 1, Yes + partial recovery = 2, Yes + full recovery = 3 | 46/481 (10%) |
| 2d. Data exfiltration | Yes = 1 / No = 0 | 60/481 (13%) |
| 2e. Yearly revenue victim | Euro, Log 10 transformed | 11/481 (2%) |
| 2f. Sector victim | Sectors described by Dutch Chamber of Commerce | 20/481 (4%) |
| 3a. Data set | IR company = 2, IR company + police = 1 Police = 0 | 0/481 (0%) |
| 3b. Year encryption | 2019, 2020, 2021, 2022 | 18/481 (4%) |

TABLE II
SECTOR SIZE IN NETHERLANDS ACCORDING TO CBS [9].

| Sector Name | Description of Companies in Sector | Dutch Sector Size (%) |
|---|---|---|
| Trade | Involves the buying and selling of goods and services. | 29.9 |
| Healthcare | Provides medical services, including hospitals and clinics. | 29.3 |
| Government | Covers public administration, defense, and social services. | 12.1 |
| Education | Includes schools, colleges, and educational services. | 11.8 |
| Construction | Concerns the building of infrastructure and buildings. | 8.6 |
| Transport | Involves the movement of goods and people. | 8.5 |
| Leisure | Includes recreation, entertainment, and tourism. | 6.8 |
| ICT | Focuses on Information and Communication Technology services. | 5.2 |
| Media | Covers broadcasting, publishing, and other forms of media dissemination. | 5.2 |
| Agriculture | Involves farming, forestry, and fishing. | 2.1 |

**1b.** *Payment:* This binary variable indicates whether victims paid the ransom or not. It is categorized as follows: yes = 1, no = 0.

**1c.** *Ransom paid:* This variable is the primary focus of our study, measured in euros. This variable is calculated by multiplying the payment (*1c.Payment*) with the final ransom (*1b.Ransom requested end of negotiations*). If the ransom requested after the end of negotiations was unknown and there was no payment, then the ransom paid was recorded as 0.

The **independent variables** in this study (See Table I) are:

**2. Victim Characteristics:** This section examines various characteristics of the victim that could serve as significant indicators for the ransom amount paid. These characteristics align closely with our research hypotheses.

**2a.** *Time Negotiating:* The number of hours devoted to negotiations. If no negotiations occurred, the value for time negotiating was recorded as 0.

**2b.** *Insurance:* A binary variable indicating whether the victim has insurance coverage that includes ransomware attacks. Categories are defined as follows: yes = 1, no = 0.

**2c.** *Backups:* This categorical variable represents the presence of backups and their state in the event of a ransomware attack. It is categorized as follows: no = 0, yes but not possible to recover data = 1, yes but could partially recover data = 2, yes and could fully recover data = 3.

**2d.** *Data Exfiltration:* This binary variable indicates whether data from the victim was exfiltrated during the ransomware attack. It is categorized as follows: yes = 1, no = 0. Note that although many ransomware groups claim to exfiltrate data as a means of pressuring victims, most groups do not actually carry out this action [27]. Data exfiltration is documented as confirmed if in-depth analysis of network logs reveals significant and abnormal data uploading activity. Additionally, if the victim's data is found to be published on a leak page and verified as belonging to the victim, it is also categorized as data exfiltration.

**2e.** *Yearly Revenue Victim:* This variable represents the annual revenue of the victim's company, measured in euros and log-transformed, due to very skewed data [25]. The data was obtained from various public sources, including ZoomInfo and DnB [22]. It is worth noting that these sources are also utilized by criminals to access the yearly revenue information of their targets. While there may be inaccuracies in the data retrieved from these sources, its usage by criminals provides a relevant basis for examining potential price discrimination strategies.

**2f.** *Sector Victim:* This categorical variable identifies the economic sector to which the victim's company belongs,

based on the categories employed by the Dutch Chamber of Commerce [9]. See Table II.

**3. Contextual Variables:** This section highlights the inclusion of metadata which might influence the ransom paid.

**3a.** *Data set:* A categorical variable indicating the origin of the attack data, categorized as police data set, IR company data set, or both.

**3b.** *Year encryption:* A categorical variable indicating the year when encryption of victim's files occurred, limited to 2019, 2020, 2021, or 2022.

As ransom paid is the primary focus of our study, we have employed a listwise deletion approach for the regression analysis, removing all cases where the amount of ransom payment was unobserved, resulting in 430 ransomware cases for descriptive analysis. Similarly, applying listwise deletion for the other variables (as depicted in Table I), resulted in 382 observation for the regression analysis. Although using a different sample size for descriptive and regression analysis might make it harder to compare results, we want our analysis to be as close to the real-life data as possible. Likewise, the listwise deletion approach could introduce potential bias if the ransom payment data is not missing-at-random [33]. However, the method aligns with our research objectives, since we only want to analyse observed ransom payments and the amount of missing observations is relatively low, less than $10\%$.

Analysis were conducted using Rstudio and R version 4.3.1, with packages *pscl*, *ggplot* and *dplyr*.

We adopt a two-step approach to model the ransom paid in our study, utilizing a hurdle model as proposed by [29]. The hurdle model is suitable for capturing the decision-making process of ransom payment, with the "hurdle" representing the likelihood of a victim paying the ransom, and only after overcoming this hurdle, positive ransom payments are observed. This framework combines two components: the first models the probability of attaining a ransom paid or no payment, while the second part models the ransom amount given that the ransom payment is non-zero. Hurdle models give extra insight by capturing factors influencing zeroes and factors influencing positive amounts [13], [18]. The advantage of using a hurdle model is that it could handle excess zeros efficiently [18]

In our analysis, we employ a hurdle model with a negative binomial distribution. This distribution allows us to model the ransom paid while relaxing the assumption of equal mean and variance as would be the case using a Poisson Distribution. Furthermore, we use a Log Link function to model the logarithm of ransom paid. Log-transforming variables with monetary scales is common in social-empirical studies to transform a non-linear distributed variable to an approximately normal distributed variable [25], [37]. The probability of a victim making no payment can be represented as follows:

$$P(Y_i = 0) = \frac{1}{1 + e^{-\lambda}} \tag{1}$$

Where $Y_i$ is the ransom amount $Y$ paid by victim $i$ and the parameter $\lambda$ is used to predict the count of zero ransom payments. The probability of a non-zero ransom amount, conditional on payment of ransom amount $y > 0$ is:

$$P(Y_i = y) = \frac{\Gamma(y + r_i)}{y! \cdot \Gamma(r_i)} \left(\frac{r_i}{r_i + \mu_i}\right)^{r_i} \left(\frac{\mu_i}{r_i + \mu_i}\right)^{y} \tag{2}$$

With $r_i$ is the dispersion parameter for victim $i$ and $\mu_i$ is the mean parameter for victim $i$.

We model the expected ransom amount when a victim pays a ransom as:

$$E(Y_i | Y_i > 0) = e^{\beta_0 + \beta_1 x_i} \tag{3}$$

With $x_i$ the relevant covariate for victim $i$, and $\beta_0$ and $\beta_1$ regression coefficients. Using the probability distributions (1) and (2) we could extract the total expected ransom amount for both victims who pay and who do not.

$$E(Y_i) = P(Y_i > 0) \times E(Y_i | Y_i > 0) \tag{4}$$

Equation (4) allows us to construct a regression model that accounts for multiple regressors, enabling us to evaluate their effect on ransom paid. With this regression model, we seek to validate the previously stated hypotheses. We set the significance level to $\alpha = 0.05$, and a p-value below this threshold supports the hypothesis that the variable is significant.

## IV. Results

### A. Descriptive Analysis

In this subsection we first examine the cumulative, average, and frequency of ransom payments in relation to the various variables outlined in Section III. Subsequently, we will conduct a detailed analysis of the characteristics specific to victim companies across different sectors. For an overview of our results, please refer to Tables III and IV.

Among the 430 victims, 121 victims decided to proceed with ransom payment, approximately $28\%$. Regarding the total ransom payments made, the combined sum in our data set amounts to 50,427,252 euros. For those who chose to pay, the average ransom amount was 431,002 euros, with a median of 35,000 euros. See Figure 2 for the distribution of ransom paid. The distribution seems to be lognormal distributed, but not uniform, which might contradict that criminals in this dataset use uniform pricing.

In 2020 a substantial sum of approximately 28 Million euros ransom was paid, marking an increase compared to the preceding year when the ransom payment amounted to 312,053 euros. This rise in ransom payments can be attributed not only to an increase in the number of attacks (84 in 2019 and 113 in 2020) but also to a higher average ransom paid per attack. However, in subsequent years, namely 2021 and 2022, the ransom payments decreased to around 12 Million and 11 Million euros, respectively. A Kruskal-Wallis test, which is a non-parametric test with the null hypothesis that in all years the ransom paid is the same, results in KW=8.825, df=3, p-value=0.03. This implies that at least in one year the ransom paid is different compared to other years.

TABLE III
SUM AND AVERAGE RANSOM PAID FOR DIFFERENT VARIABLES. N=430.

| | Categories | # Paid | # Not Paid | Sum Ransom Paid (euro) | Average Ransom Paid (euro) |
|---|---|---|---|---|---|
| Year | 2019 | 16 (19%) | 68 (81%) | 312,053 | 19,503 |
| | 2020 | 39 (35%) | 74 (65%) | 27,629,373 | 708,445 |
| | 2021 | 37 (28%) | 94 (72%) | 11,848,461 | 320,229 |
| | 2022 | 25 (27%) | 67 (73%) | 10,637,366 | 425,495 |
| Insurance | No | 75 (24%) | 232 (76%) | 9,976,185 | 133,016 |
| | Yes | 33 (44%) | 42 (56%) | 23,367,453 | 708,105 |
| Backups | No | 28 (27%) | 76 (73%) | 1,417,017 | 50,608 |
| | Yes, but not recoverable | 45 (58%) | 33 (42%) | 16,251,606 | 361,147 |
| | Yes, but partially recoverable | 24 (28%) | 63 (72%) | 11,706,451 | 487,769 |
| | Yes, and fully recoverable | 13 (11%) | 109 (89%) | 19,671,327 | 1,513,179 |
| Data exfiltration | No | 82 (25%) | 250 (75%) | 7,331,363 | 89,407 |
| | Yes | 35 (40%) | 53 (60%) | 43,095,889 | 1,231,311 |
| Data set | Police | 71 (21%) | 263 (79%) | 21,087,499 | 301,250 |
| | Police and IR company | 18 (52%) | 16 (48%) | 9,460,831 | 556,520 |
| | IR company | 32 (52%) | 30 (48%) | 19,878,922 | 662,631 |
| Total | | 121 (28%) | 309 (72%) | 50,427,252 | 431,002 |

TABLE IV
DESCRIPTIVE STATISTICS OF VICTIM COMPANIES OF DIFFERENT SECTORS. MEAN AND MEDIAN REVENUE ARE IN MILLION EUROS, INSURED, NO BACKUP, AND PAID ARE PERCENTAGES. AVERAGE RANSOM PAID IS IN EURO AND CUMULATIVE RANSOM PAID IS IN MILLION EUROS. BOTTOM ROW DEMONSTRATES UNWEIGHTED COLUMN AVERAGE. N=430.

| | Sector | Number attacks | Number attacks (%) | CBS Sector Size (%) | Mean Revenue (Meuro) | Median Revenue (Meuro) | Insured (%) | No Backup (%) | Paid (%) | Average Ransom Paid (euro) | Cumulative Ransom Paid (Meuro) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Trade | 140 | 32.6 | 29.9 | 301.91 | 4.07 | 19.4 | 46.8 | 30.7 | 112,793 | 15.79 |
| 2 | Construction | 77 | 17.9 | 8.6 | 382.30 | 4.47 | 28.8 | 48.0 | 28.6 | 46,676 | 3.59 |
| 3 | ICT | 63 | 14.7 | 5.2 | 397.08 | 3.81 | 19.7 | 46.6 | 28.6 | 268,039 | 16.89 |
| 4 | Healthcare | 29 | 6.7 | 29.3 | 37.44 | 3.61 | 19.2 | 37.9 | 32.1 | 94,784 | 2.75 |
| 5 | Leisure | 29 | 6.7 | 6.8 | 7.55 | 1.24 | 22.2 | 59.3 | 24.1 | 31,934 | 0.93 |
| 6 | Transport | 27 | 6.3 | 8.5 | 490.40 | 5.82 | 7.7 | 64.0 | 33.3 | 102,690 | 2.77 |
| 7 | Media | 25 | 5.8 | 5.2 | 424.02 | 3.64 | 16.7 | 47.8 | 20.0 | 274,409 | 6.86 |
| 8 | Education | 14 | 3.3 | 11.8 | 107.40 | 16.87 | 0.0 | 28.6 | 21.4 | 22,138 | 0.31 |
| 9 | Agriculture | 14 | 3.3 | 2.1 | 387.61 | 0.83 | 14.3 | 53.8 | 15.4 | 12,389 | 0.17 |
| 10 | Government | 12 | 2.8 | 12.1 | 58.60 | 21.27 | 16.7 | 41.7 | 8.3 | 34,146 | 0.41 |
| | **Average** | **43** | - | - | **269.43** | **6.66** | **16.5** | **47.7** | **24.3** | **104,100** | **5.05** |

Regarding insurance, it is observed that having insurance coverage correlates with a higher likelihood of payment, with 44% of victims opting to pay when insured, as opposed to 24% when uninsured. Additionally, the average amount paid is also greater when the victim has insurance, 708,105 euros, compared to 133,016 euros for those without insurance. Consequently, the total amount of ransom paid is significantly higher for insured victims, reaching approximately 23 Million euros, in contrast to around 10 Million euros for uninsured victims. The Kruskal-Wallis test with null hypothesis that ransom paid with and without insurance is equal, results in KW=20.12, df=1, p-value$<$0.001. This indicates that having insurance leads to more ransom paid.

Regarding backups, it seems that having recoverable backups leads to a lower probability of payment, observed in only 11% of cases. However, the average ransom paid per attack and the total ransom paid are higher compared to scenarios with other backup conditions. It is noteworthy that victims who lack backups generally pay lower ransoms than those who have backups that cannot be restored, with both the average ransom per attack and the cumulative amounts being lower. One plausible explanation could be that businesses holding data considered valuable enough for ransom payments are generally more likely to employ backup systems, compared to those with less valuable data. The Kruskal-Wallis test with null hypothesis that all backups measures lead to same ransom paid, results in KW=49.65, df=3, p-value$<$0.001. This indicates that having backups leads to more ransom paid.

In relation to data exfiltration, cases involving exfiltration of data result in a higher probability of payment, as observed in 40% of such incidents, compared to 25% when no data exfiltration occurs. Additionally, the average amount paid is substantially larger, approximately 1.2 Million euros when data is exfiltrated, as opposed to 89,407 euros when no data exfiltration is confirmed. Consequently, the total ransom paid is considerably higher in cases where data exfiltration takes place, reaching approximately 43 Million euros, in contrast to approximately 7 Million euros in attacks without data exfiltration. The Kruskal-Wallis test with null hypothesis that ransom paid with and without data exfiltration is equal, results in KW=15.38, df=1, p-value$<$0.001. This indicates that data exfiltration leads to more ransom paid.

In terms of the data set used, a higher proportion of ransom payments occur in the data set of the incident response (IR)

company, accounting for 52% of cases. This percentage aligns with the combined number of payments made to both the IR company and the police. In comparison, the data set from the police shows a lower ransom payment rate of 21%.

The average annual revenue of victim companies was 269.43 Million euros (sd = 1,802 Million euros). The median revenue was 6.66 Million euros, and the geometric mean was 3.03 Million euros.

The average time spent negotiating was approximately 37 hours (sd = 92 hours). However, when considering only cases where the victim engaged in negotiations, the average negotiating time was 111 hours (sd = 131 hours). Notably, the average negotiating time was lower when a ransom was paid, approximately 25 hours (sd = 78 hours), compared to cases where no payment was made, 72 hours (sd = 118 hours).

In terms of the number of attacks across sectors, the Trade sector stands out with 140 attacks (32.56%), which seems proportionate to its CBS sector size of 29.9%, as shown in Table IV. Construction and ICT sectors follow with 77 and 63 attacks, respectively, which is particularly significant given their smaller sector sizes of 8.6% and 5.2% according to CBS data [9].

When examining the characteristics of victim companies in different sectors in Table IV, it is noteworthy that healthcare and leisure sectors have higher-than-average percentage of insured companies (22.2% and 19.2%) compared to an average of 16.5%. Victim companies in the Leisure sector have more non-recoverable backups in place than average with 59.3%. Healthcare has higher proportion of companies with recoverable backup measures in place 37.9%. Despite their good backup practices, companies in the healthcare sector pay more than average the ransom with 32.1%, Leisure is close with the average with 24.1%. However, their average and cumulative ransom payments are lower compared to other sectors. These numbers illustrate that different sectors have their own unique challenges when it comes to dealing with ransomware attacks.

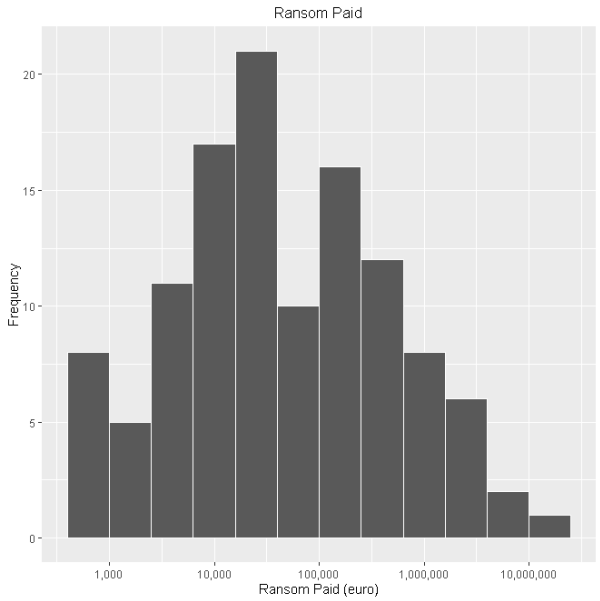


Fig. 2. Distribution of ransom paid.

On the higher end of the revenue spectrum, the Transport, Media, and ICT sectors have the largest average revenues of 490.40, 424.02, and 397.08 million euros, respectively. Transport companies are less frequently insured (7.7%) and have fewer backup systems (64%), yet pay ransoms at a considerably higher rate of 33.3% compared to the average of 24.3%. The ICT sector, despite an average rate of backup implementation (46.6%), have the highest average ransom payments of 268,039 euros on average, contributing to the largest cumulative ransom of 16.89 million euros across all sectors.

In conclusion, the ICT sector seems the most lucrative target for ransomware groups, since they pay the largest ransom per attack on average. One explanation is that ICT companies often provide critical infrastructure or services to numerous clients. Consequently, if such companies experience downtime due to a ransomware attack, it can have a cascading impact on a large number of clients, thus providing ransomware groups with greater leverage to demand larger ransoms, which aligns with the trends observed in our data set.

### *B. Demand Curve of Ransomware*

A useful concept for understanding ransom payments is a demand curve [6]. A demand curve, for any ransom amount, depicts the proportion of victims willing to pay that amount. Constructing a demand curve based on empirical observations is challenging [24], due to endogeneity: ransomware criminals might adjust the ransom amount based on the victims' response to negotiation. Consequently, the observed data represents a mixture of both the victims willingness to pay (demand side) and the criminals willingness to negotiate up or down the ransom amount, and make a deal (supply side).

To explore the willingness of victims to pay the ransom we, therefore, need to make assumptions. To motivate our assumptions consider the following stylized thought experiment: (i) During negotiations with a victim, the criminals incrementally change the ransom request until they discern maximum willingness to pay. (ii) The criminal then decides whether to accept the highest amount the victim will pay, or walk away because the ransom amount is too low (and may harm reputation in future negotiations). This means that if a victim paid the ransom then the criminals were able to fully exploit the victims willingness to pay. In reality, this will under-estimate willingness to pay because victims may have been willing to pay a higher ransom than the criminals requested. It also means that if a victim did not pay then we can assume they would have paid an amount just below the last amount requested. In reality, this will over-estimate willingness to pay.

*Assumption 1: (a) Victims who paid a ransom of $x$ euros would have paid any ransom less than $x$ but not a ransom above $x$. (b) Victims who did not pay a ransom request of $x$*

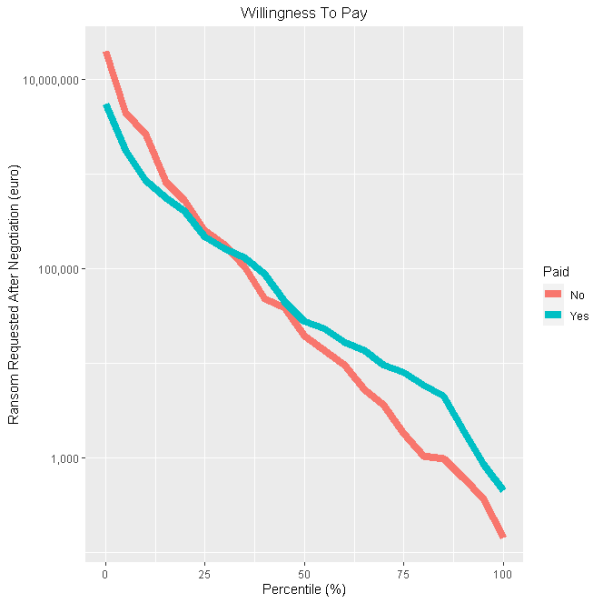


Fig. 3. Ransom amount in euros paid by victims (blue line, *yes curve*) and those who did not pay (red line, *no curve*). Ordering the data according to ransom amounts under the assumption that victims who paid would pay less and those who did not pay would not pay if the ransom is larger, results in a demand-like curve.

*euros would not pay any ransom larger than $x$ but would pay a ransom below $x$.*

Applying Assumption 1(a) we can derive an estimated demand curve for those companies that paid a ransom. For instance, considering the lowest amount paid, which is approximately 500 euros, we infer that 100% of the victims who paid were willing to pay this price. Similarly, observing that around 50% of victims paid more than 35,000 euros, we deduce that 50% of them were willing to pay this amount. Combining these results, we obtain the blue line in Figure 3. The blue line or *yes curve* is an estimate of the demand curve based solely on data derived from companies that paid the ransom. This curve is potentially biased by only including companies who paid and by potentially under-estimating the willingness to pay of companies that paid.

Applying Assumption 1(b) we can derive an estimated demand curve for those companies that did no pay a ransom. Now, the argument proceeds in the opposite direction. Here, if we observe, say, 65% of companies refusing to pay a ransom request of $100,000$ euros or below, then we infer that 35% of companies would have be willing to pay a ransom of $100,000$. This aggregation yields the red line in Figure 3. This estimated demand curve is potentially biased by only including those who did not pay and by potentially over-estimating the willingness to pay of those who did not pay.

While the two estimated demand curves in Figure 3 are derived using stylized assumptions they both give a similar picture of the underlying demand curve. The *yes curve* gives a higher estimate of demand at low ransoms because it is based on those who paid. The *no curve* gives a higher estimate of demand at very high ransoms because it includes observations with very high ransoms that were not paid. In both cases, though, we see an approximate log-linear relationship between willingness to pay and demand with around 35% willing to pay a ransom of $100,000$ euros.

### C. Hurdle Model of Ransom Paid

The results of the hurdle model are described in Table V. The dispersion parameter is significant, which implies the negative binomial distribution is the appropriate fit.

The findings of this study provide empirical support for the confirmation of H1, indicating that distinct factors influence the decision-making process concerning ransom payments compared to the actual ransom amount paid. Specifically, instances involving victims who hire an Incident Response (IR) company ($\beta$=3.19, p<0.001) or both the IR company and the police ($\beta$=2.32, p<0.001) demonstrate higher payment rates than those solely reporting to the police, which validates hypothesis H2.1. However, contrary to hypothesis H2.2, victims with assistance from IR companies ($\beta$=0.36, p=0.49) and the data set involving both the police and IR company ($\beta$=0.71, p=0.19) did not pay larger ransoms.

Regarding insurance coverage, victims with insurance do not appear to be more inclined to pay the ransom (H3.1) ($\beta$=-0.23, p=0.61). Nonetheless, they do pay larger ransom amounts, thus confirming hypothesis H3.2 (insurance coverage $\beta$=1.03, p<0.001). Taking the exponential of $\beta$ leads to 2.7, which indicates that insurance leads to 2.7 times larger ransom paid.

The presence of recoverable backups significantly diminishes the likelihood of payment (H4.1), as follows from reduced probability of ransom payments when victims have partially ($\beta$=-0.87, p=0.04) or fully recoverable backups ($\beta$=-3.31, p<0.001). However, recoverable backups do not appear to influence the ransom amount paid (H4.2).

Data exfiltration does not lead to more frequent ransom payments (H5.1) ($\beta$=0.26, p=0.54); nonetheless, it does result in a larger ransom amount paid (H5.2), as supported by the positive relationship between data exfiltration and the ransom amount paid ($\beta$=1.49, p<0.001). Taking the exponential of $\beta$ leads to 4.4, which indicates that data exfiltration leads to 4.4 times larger ransom paid.

The log yearly revenue of the victim does not appear to impact the decision to pay the ransom (H6.1) ($\beta$=0.12, p=0.29). However, it does lead to larger ransom payments, which confirms hypothesis H6.2 (log yearly revenue of the victim $\beta$=0.39, p<0.001). Since both the dependent and independent variable are logarithms, we could interpret the $\beta$ as the elasticity: an 1% increase in a victim's yearly revenue causes a 0.12% rise in the ransom paid.

Lastly, the frequency of ransom payments did not change over the four years (H7.1). However, the ransom paid during 2020 and 2021 exceeded that of 2019 and 2022 (H7.2). Notably, ransom payments were higher in 2020 ($\beta$=1.02, p=0.02) and 2021 ($\beta$=1.21, p=0.02) compared to 2019. Table

TABLE V

HURDLE MODEL. THE ZERO HURDLE MODEL AT THE BOTTOM MODELS THE FIRST STEP WHETHER VICTIMS DECIDE TO PAY OR NOT. THE COUNT MODEL MODELS THE SECOND STEP HOW MUCH RANSOM A VICTIM PAYS IF THE VICTIM DECIDES TO PAY IN THE FIRST STEP. ESTIMATE, STD. ERROR AND Z-VALUE ARE ROUNDED TO TWO DECIMALS, P-VALUE TO THREE DECIMALS. N = 382.

| **Second Step: Count Model** | **Estimate** | **Std. Error** | **z-value** | **p-value** | **Sign.** |
|---|---|---|---|---|---|
| Intercept | 6.88 | 0.84 | 8.17 | 0.000 | *** |
| Year = 2020 | 1.02 | 0.43 | 2.37 | 0.018 | * |
| Year = 2021 | 1.21 | 0.53 | 2.28 | 0.023 | * |
| Year = 2022 | -0.05 | 0.59 | -0.09 | 0.931 | |
| Insurance = Yes | 1.03 | 0.29 | 3.60 | 0.000 | *** |
| Log Yearly Revenue Victim | 0.39 | 0.09 | 4.49 | 0.000 | *** |
| Backups = Yes, not recoverable | 0.12 | 0.36 | 0.33 | 0.741 | |
| Backups = Yes, partially recoverable | 0.32 | 0.46 | 0.70 | 0.485 | |
| Backups = Yes, fully recoverable | 0.51 | 0.52 | 1.00 | 0.320 | |
| Data exfiltration = Yes | 1.49 | 0.37 | 4.02 | 0.000 | *** |
| Data set = IR company + Police | 0.71 | 0.54 | 1.30 | 0.193 | |
| Data set = IR company | 0.36 | 0.52 | 0.69 | 0.491 | |
| $\text{Log}(\text{r}_i)$ | -0.28 | 0.12 | -2.31 | 0.021 | * |
| **First Step: Zero Hurdle Model** | **Estimate** | **Std. Error** | **z-value** | **p-value** | **Sign.** |
| Intercept | -1.99 | 0.74 | -2.67 | 0.008 | ** |
| Year = 2020 | 0.82 | 0.40 | 2.05 | 0.040 | * |
| Year = 2021 | -0.10 | 0.44 | -0.23 | 0.819 | |
| Year = 2022 | 0.09 | 0.52 | 0.18 | 0.859 | |
| Insurance = Yes | -0.23 | 0.45 | -0.52 | 0.606 | |
| Log Yearly Revenue Victim | 0.12 | 0.11 | 1.06 | 0.290 | |
| Backups = Yes, not recoverable | 0.62 | 0.36 | 1.70 | 0.090 | |
| Backups = Yes, partially recoverable | -0.87 | 0.42 | -2.06 | 0.039 | * |
| Backups = Yes, fully recoverable | -3.31 | 0.61 | -5.44 | 0.000 | *** |
| Data exfiltration = Yes | 0.26 | 0.42 | 0.61 | 0.544 | |
| Data set = IR company + Police | 2.32 | 0.62 | 3.72 | 0.000 | *** |
| Data set = IR company | 3.19 | 0.67 | 4.75 | 0.000 | *** |

[1] Where Sign. is $^{*}\text{p} \leq .05$, $^{**}\text{p} \leq .01$, $^{***}\text{p} \leq .001$.

VI provides an overview which hypotheses are confirmed or rejected.

## V. DISCUSSION AND CONCLUSION

The present study set out to examine the ransom paid during ransomware attacks, analyzing 382 ransomware incidents reported to the Dutch Police and an IR company in the Netherlands. Drawing on economic literature, we proposed a two-step process that determines the ransom amount paid. Initially, victims decide whether to pay, followed by the decision of how much to pay, which we modeled using a hurdle model. Our model focused on personalized ransom pricing by ransomware criminals, since is most common for businesses and organizations, compared to individuals who more often encounter uniform pricing [26]. Our estimated hurdle model revealed distinct factors influencing each decision.

Our first research question focused on the first step in the two-step process: factors determining whether victims will pay the ransom. Our findings suggest that the decision to pay depends on backups measures and companies who hire an IR company. Furthermore, there was a difference in frequency of paying the ransom in 2020 compared to the other years examined in this study. Insurance, yearly revenue and data exfiltration do not seem to influence the victims' decision to pay the ransom.

Our second research question focused on the factors determining how much ransom will pay, the second step of our two-step process. Our findings suggest that data exfiltration, insurance coverage and yearly revenue of the victim are important factors for determining how much ransom a victim will pay if they decide to pay. Furthermore, in 2020 and 2021 more ransom was paid than in 2019 and 2022. We did not find differences in ransom paid between victims with different backups measures and companies in the IR company data set.

Our third research question focused on whether the decision to pay and ransom amount paid depend on distinct factors. Based on the findings from the previous two research questions, we can conclude different factors influence the two steps in our model. Furthermore, the hurdle model supports the notion of a two-step choice process proposed by [11]. Companies first assess affordability and then evaluate the advantages and disadvantages of paying versus pursuing alternative data retrieval methods to minimize disruption and financial losses.

The significance of backups for the decision to pay ransom aligns with the rationale that having an alternative recovery procedure is crucial in avoiding costly downtime, in line with [17]. Additionally, our analysis showed that companies consulting the IR company were more willing to pay, as they sought guidance expert assistance in recovering from the ransomware attack. In case the victim considered payment, the IR company helps navigating the payment process, understanding associated risks, and potentially negotiating a discount on the ransom, as outlined by [40].

Previous research already addressed that insurance does not necessarily increase the probability of ransom payments [7] as was confirmed by our results. Nevertheless, having insurance

TABLE VI
SUMMARY OF RESULTS FOR DIFFERENT HYPOTHESES. THE SIGN DENOTES THE TYPE OF RELATIONSHIP, POSITIVE +, NEUTRAL = AND NEGATIVE -. CONFIRMED HYPOTHESIS HAVE A ✓, WHEREAS REJECTED HYPOTHESES HAVE A -.

| Variable | Sign | Hypothesis | Confirmed |
|---|---|---|---|
| H1: Two-step approach | = | Different factors influence ransom paid and payment decision | ✓ |
| H2: IR company and police | + | H2.1: Pay or not | ✓ |
| | + | H2.2: Ransom amount | - |
| H3: Insurance | + | H3.1: Pay or not | - |
| | + | H3.2: Ransom amount | ✓ |
| H4: Recoverable Backups | - | H4.1: Pay or not | ✓ |
| | = | H4.2: Ransom amount | - |
| H5: Data Exfiltration | + | H5.1: Pay or not | - |
| | + | H5.2: Ransom amount | ✓ |
| H6: Yearly Revenue | + | H6.1: Pay or not | - |
| | + | H6.2: Ransom amount | ✓ |
| H7: Year encryption | = | H7.1: Pay or not | - |
| | + | H7.2: Ransom amount | ✓ |

does lead to larger ransom paid. Perhaps this is due to exposed moral hazard: since someone else is paying for the victim, the victim is willing to pay a larger amount. However, exposed moral hazard would also imply a larger proportion of victims be willing to pay the ransom. Perhaps ethical considerations or partial coverage by insurance might explain this difference in our results.

Likewise, the yearly revenue of a company did not influence the payment decision, but did influence the ransom paid. This result is in line with [19], [25]. This might due to victims being more financially capable to pay larger ransom and price discrimination strategies from the criminals [6], [19].

Contrary to prior claims [23], [27], data exfiltration did not directly lead to increased probability of ransom payments. However, our study found that victims tend to pay more when data exfiltration occurred, potentially to avoid reputation costs linked to data publication. The difference in findings may arise from using a hurdle model: although the payment rates are significantly larger with data exfiltration than without, controlling for all other variables this difference seems to be insignificant. This finding illustrates the power a hurdle model: simultaneously estimating proportion paying and ransom amount paid.

Our results show that ransom payments in 2020 and 2021 are different from other years, which is congruent with previous findings [10], [12]. Perhaps, ransom payments in 2021 are influenced by major global events. Economically, the year was marked by the COVID-19 pandemic and the initial stages of the Ukraine conflict [35]. These events, coupled with evolving cyber insurance policies, such as Lloyd's exclusion clauses, may have impacted ransomware payment strategies. While our analysis suggests these factors as possible influences, it is important to note that it is impossible to be certain, given the complex interaction between global economic, political dynamics, and cybercrime."

It is often assumed that the willingness to report ransomware attacks to the police is typically low [25]. However, our investigation, which involved comparing data from the police and an IR company, revealed a notably high reporting rate of 62% among Dutch companies. This proportion exceeds the rates of 8-10% reported in studies focusing on the willingness to report online fraud cases to the Dutch Police [36]. This difference in reporting behavior could be attributed to victims being more inclined to report severe crimes to the police [34]. Even though our data set is limited to one IR company, the high reporting rate among Dutch companies is unlikely to be affected by lower willingness to report from victims managed by other IR companies, considering that the IR company featured in the present study accounted for half of the victims managed by any IR company in the Netherlands [27].

Nevertheless, it is good to mention that differences between the police and IR company data sets might be the result of internal processing of information and data. Typically, data from the police was unstructured and incomplete, whereas data from the IR company was typically more structured and complete. The differences found between the two data sets might be the result of this difference in data collection, processing and storage.

In conclusion, this study provides valuable insights into victim's decision-making process of paying the ransom during ransomware attacks. We analyzed 382 ransomware attacks reported to the Dutch Police and to an IR company, controlling for reporting bias. Our findings reveal a two-step process in ransom payments, with distinct factors influencing the decision to pay and the amount paid. These contributions aid in developing effective strategies to combat and mitigate the impact of ransomware attacks.

## VI. LIMITATIONS AND FURTHER WORK

Limitations of this study include:

1) Our study focused mostly on companies in the Netherlands. It might be difficult to generalize our results to other countries. In other countries ethical considerations of paying the ransom might be different than the Netherlands, possibly changing the significance and/or effect size of different factors influencing the two different steps in our study [14]. However, due to the sensitivity of the data, it might be hard to get data from other countries.
2) In our models we did not account for the perceived reputation of the attacker, which could significantly impact victim decisions on payment and ransom amount. Here reputation is the perceived probability of getting a key to regain access to files after payment [5].
3) Due to the sensitive nature of the data, only one person could code the data, see also [25]. This may introduce different types of biases, despite efforts to mitigate these biases through anonymous group discussions.
4) The potential endogeneity of ransom price on the decision to pay was outside the scope of the present paper. As the ransom requested may influence victim willingness to pay, criminals could adjust the ransom amount to maximize their profits. The potential supply-side of the demand curve could be modeled with endogeneity models [24].

Future research can explore several interesting avenues. Firstly, a focus on studying the endogeneity of price and willingness to pay could enhance our understanding of the dynamic between ransom requested and ransom paid. Secondly, accounting for the perceived trustworthiness of the attacker may influence the decision-making process, probably affecting both the likelihood of payment and the ransom amount. Lastly, generalizing the study's results to more countries could offer insights into potential variations in factors influencing the two steps, leading to more effective policy-making and a broader understanding of ransomware attack profitability.

This study provides valuable insights for policy makers and law enforcement in devising interventions to combat ransomware profitability. Two approaches can be considered:

1) Focus on the first step of the hurdle model: Encourage fewer victims to pay by emphasizing the importance of having recoverable backups. Promoting offline backups and conducting ransomware attack simulations can help prevent hasty decisions to pay.
2) Address the second step of the hurdle model: If victims decide to pay, they should pay less. Measures could include encouraging companies to take preventive measures against data exfiltration and engaging with cyber insurance companies to strategize on handling ransomware payments. Targeting large companies first in awareness campaigns may prove effective, as their refusal to pay can undermine ransomware profitability compared to smaller businesses.

In assessing the role of insurance providers in the ransomware economy, it's crucial to recognize that the current financial incentives might not encourage these companies to minimize ransom payments. In many instances, paying the ransom is the least costly option from a short-term perspective. This raises important questions about the need for regulatory intervention to correct what could be considered a market failure.

From a policy standpoint, several options are possible. One could consider a ban on insurance companies covering ransom payments. However, this may have no effect if an insurance payout still gives the company sufficient financial leverage to cover to the ransom themselves. Another possibility would be to restrict insurance payouts if a victim makes a ransom payment. However, this might lead to more companies going bankrupt, since they might not afford the ransom requested and also could not recover without the decryption key. Therefore it is important to consider the social welfare consequences of such a policy intervention.

Moreover, insurance companies could contribute to the fight against ransomware by increasing transparency and sharing valuable data with law enforcement. By doing so, we can collectively develop a richer understanding of the ransomware ecosystem, leading to better-informed strategies for combating these threats.

In conclusion, our recommendation is to consider more nuanced changes to insurance policies. These could offer a more effective approach for reducing the societal cost of ransomware attacks than more heavy-handed interventions like outright bans or additional taxes on ransom payments.

## VII. Ethics

We follow the principles from Menlo Report [2] to justify the ethical considerations made in this study:

**Respect for Persons:** Privacy and confidentiality of participants were prioritized. Individual cases were not considered, and data were aggregated at the sector levels to ensure the privacy of victims.

**Beneficence:** To maximize benefits and minimize harm, access to police investigation information was restricted to one member of the project with security clearance, while other team members received aggregated results. This approach, despite challenges to transparency, was deemed necessary for the large-scale empirical ransomware study. Additionally, understanding victims' decision-making about ransom payments may inform future criminals. Our research adheres to the principle of full-disclosure. Considering the entire study, we estimate that our model better informs victims and policy makers how to take preventive measures to prevent further harm than it educates criminals.

**Justice:** Equal opportunity was ensured for all ransomware attacks in the study, as selection was based solely on the keyword "ransomware" in police systems and attacks disclosed by the IR company. No additional emphasis was given to attacks with media attention or those involving the IR company.

**Respect for Law and Public Interest:** Specific information about certain groups, strains, or Dutch Police operations

was excluded from the paper. Additionally, the IR company was involved in reviewing the paper to exclude potentially malicious information. The goal of the study is to inform potential victims and policy makers to take effective preventive measures.

## REFERENCES


[1] Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M. & Savage, S. (2013). Measuring the cost of cybercrime. The economics of information security and privacy, 265-300.

[2] Bailey, M., Dittrich, D., Kenneally, E., & Maughan, D. (2012). The menlo report. IEEE Security & Privacy, 10(2), 71-75.

[3] Balasubramanian, A. (2021). Insurance against ransomware. Available at SSRN 3846111.

[4] Bischoff, P. (2022). Ransomware attacks cost the US $159.4bn in downtime alone in 2021. Comparitech. https://www.comparitech.com/blog/information-security/us-ransomware-attacks-cost/

[5] Cartwright, A., & Cartwright, E. (2019). Ransomware and reputation. Games, 10(2), 26.

[6] Cartwright, E., Hernandez Castro, J., & Cartwright, A. (2019). To pay or not: game theoretic models of ransomware. Journal of Cybersecurity, 5(1), tyz009.

[7] Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. (2023). How cyber insurance influences the ransomware payment decision: theory and evidence. The Geneva Papers on Risk and Insurance-Issues and Practice, 48(2), 300-331.

[8] Cartwright, A., Cartwright, E., Xue, L., & Hernandez-Castro, J. (2023). An investigation of individual willingness to pay ransomware. Journal of Financial Crime, 30(3), 728-741.

[9] CBS (2023). Table on employees by sector and size of company. Retrieved August 22, 2023, from https://opendata.cbs.nl/statline/#/CBS/en/dataset/84985ENG/table

[10] Chainalysis. (2023). Crypto Ransomware Revenue Down as Victims Refuse to Pay. Retrieved July 23, 2023, from https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/

[11] Connolly, A. Y., & Borrion, H. (2022). Reducing ransomware crime: analysis of victims' payment decisions. Computers & Security, 119, 102760.

[12] Coveware. (2023). Ransom Monetization Rates Fall to Record Low Despite Jump in Average Ransom Payments. Coveware Blog. Retrieved July 25, 2023, from https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

[13] Cragg, J. G. (1971). Some statistical models for limited dependent variables with application to the demand for durable goods. Econometrica: journal of the Econometric Society, 829-844.

[14] Culafi, A. (2023, July 24). Coveware: Rate of victims paying ransom continues to plummet. TechTarget. Retrieved August 22, 2023, from https://www.techtarget.com/searchsecurity/news/366545539/Coveware-Rate-of-victims-paying-ransom-continues-to-plummet

[15] Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. Luxembourg: Publications Office of the European Union. Retrieved August 31, 2023, from https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

[16] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg, Retrieved August 31, 2022, from https://www.europol.europa.eu/publications-events/mainreports/internet-organised-crime-threat-assessment-iocta-2021

[17] Galinkin, E. (2021). Winning the Ransomware Lottery: A Game-Theoretic Approach to Preventing Ransomware Attacks. In International Conference on Decision and Game Theory for Security (pp. 195-207). Cham: Springer International Publishing.

[18] Greene, W. H. (2003). Econometric analysis. Pearson Education India.

[19] Hack, P., & Wu, Z. Y. (2021). We wait, because we know you. Inside the ransomware negotiation economics. NCC Group.

[20] Hassan, N. (2019). Ransomware revealed. Berkeley: Apress.

[21] Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. Royal Society open science, 7(3), 190023.

[22] Intel 471. (2022). Conti leaks: Cybercrime fire team. Intel 471. Retrieved July 24, 2023, from https://intel471.com/blog/conti-leaks-cybercrime-fire-team

[23] Li, Z., & Liao, Q. (2020). Ransomware 2.0: to sell, or not to sell a game-theoretical model of data-selling ransomware. In Proceedings of the 15th International Conference on Availability, Reliability and Security (pp. 1-9).

[24] MacKay, A., & Miller, N. (2023). Estimating models of supply and demand: Instruments and covariance restrictions. Harvard Business School Strategy Unit Working Paper, (19-051).

[25] Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. In 2022 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-13). IEEE.

[26] Meurs, T., Junger, M., Tews, E., & Abhishta, A. (2022). NAS-ransomware: hoe ransomware-aanvallen tegen NAS-apparaten verschillen van reguliere ransomware-aanvallen. Tijdschrift voor Veiligheid 21(3-4):69-88. https://doi.org/10.5553/TvV/.000044

[27] Meurs, T., & Holterman, L. (2022). Whitepaper data-exfiltratie bij een ransomware-aanval. Cyberveilig Nederland. Retrieved from https://executivefinance.nl/wp-content/uploads/2023/01/VCNL-Whitepaper-Exfiltratie.pdf

[28] Meurs, T., Junger, M., Abhishta, A., Tews, E., & Ratia, E. (2022). CO-ORDINATE: A model to analyse the benefits and costs of coordinating cybercrime. JISIS, 12(4).

[29] McDowell, A. (2003). From the help desk: hurdle models. The Stata Journal, 3(2), 178-184.

[30] Mott, G., Turner, S., Nurse, J. R., MacColl, J., Sullivan, J., Cartwright, A., & Cartwright, E. (2023). Between a rock and a hard (ening) place: Cyber insurance in the ransomware era. Computers & Security, 128, 103162.

[31] Oosthoek, K., Cable, J., & Smaragdakis, G. (2022). A tale of two markets: Investigating the ransomware payments economy. arXiv preprint arXiv:2205.05028.

[32] Pattnaik, N., Nurse, J. R., Turner, S., Mott, G., MacColl, J., Huesch, P., & Sullivan, J. (2023, July). It's more than just money: The real-world harms from ransomware attacks. In International Symposium on Human Aspects of Information Security and Assurance (pp. 261-274). Cham: Springer Nature Switzerland.

[33] Pepinsky, T. B. (2018). A note on listwise deletion versus multiple imputation. Political Analysis, 26(4), 480-488.

[34] Tolsma, J., Blaauw, J., & Te Grotenhuis, M. (2012). When do people report crime to the police? Results from a factorial survey design in the Netherlands, 2010. Journal of experimental criminology, 8, 117-134.

[35] Teichmann, F., Boticiu, S. R., & Sergi, B. S. (2023). The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate?. International Cybersecurity Law Review, 1-22.

[36] Van de Weijer, S. G., Leukfeldt, R., & van der Zee, S. (2021). Cybercrime reporting behaviors among small-and medium-sized enterprises in the Netherlands. In Cybercrime in Context: The human factor in victimization, offending, and policing (pp. 303-325). Cham: Springer International Publishing.

[37] Wang, K., Pang, J., Chen, D., Zhao, Y., Huang, D., Chen, C., & Han, W. (2021). A large-scale empirical analysis of ransomware activities in bitcoin. ACM Transactions on the Web (TWEB), 16(2), 1-29.

[38] Wolff, J. (2022). Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks. MIT Press.

[39] Wood, T., Cecchet, E., Ramakrishnan, K. K., Shenoy, P., Van der Merwe, J., & Venkataramani, A. (2010). Disaster recovery as a cloud service: Economic benefits & deployment challenges. In 2nd USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 10).

[40] Woods, D. W., Böhme, R., Wolff, J., & Schwarcz, D. (2023). Lessons lost: Incident response in the age of cyber insurance and breach attorneys. In Proceedings of the 32nd USENIX Security Symposium, Anaheim, California.