Examining ransomware payment decision-making among small and medium-sized enterprises

Sifra R. Matthijsse (ORCID ID: 0000-0002-7325-0735)[1]*

Asier Moneva (ORCID ID: 0000-0002-2156-0213)[1,2]

M. Susanne van 't Hoff-de Goede (ORCID ID: 0000-0003-0758-0143)[1]

E. Rutger Leukfeldt (ORCID ID: 0000-0002-3051-0859)[1,2,3]

AFFILIATIONS

[1] Centre of Expertise Cyber Security, The Hague University of Applied Sciences, The Netherlands.

[2] Netherlands Institute for the Study of Crime and Law Enforcement, The Netherlands.

[3] Institute of Security and Global Affairs and Institute of Criminal Law and Criminology, Leiden University, The Netherlands.

CORRESPONDENCE

Sifra R. Matthijsse. E-mail: S.R.Matthijsse@hhs.nl. Centre of Expertise Cyber Security, The Hague University of Applied Sciences, Johanna Westerdijkplein 75, 2521 EN, The Hague, The Netherlands.

PUBLISHER'S VERSION

The version of record of this manuscript is published in the European Journal of Criminology, and can be found at: https://journals.sagepub.com/doi/10.1177/14773708241285671

ABSTRACT

Ransomware is currently one of the most prominent cyberthreats for organizations. Small and medium-sized enterprises are particularly vulnerable to ransomware victimization and more inclined towards paying the ransom. However, while a few studies have been conducted on victimization of ransomware, little is known about how small and medium-sized enterprises respond to victimization and what factors contribute to the decision to pay the ransom. This study uses a survey with a vignette experiment conducted among 445 owners and managers of Dutch small and medium-sized enterprises, to gain more insight into the factors that are related to the decision to pay the ransom in the event of ransomware victimization. Findings show that the likelihood that the ransom is paid is low. While the affordability of the ransom demand seems unrelated to the likelihood of paying, being advised by a cybersecurity company to pay the ransom and not having a back-up significantly increases the likelihood of the ransom being paid. The findings provide insight into factors that make ransomware victims vulnerable to extortion. Furthermore, implications for how ransomware attacks can be mitigated are discussed.

KEYWORDS

Cybercrime; Ransomware; Victimization; Vignette

1. INTRODUCTION

Today’s society can be characterized by a high level of digitalization, with individuals and organizations increasingly spending time online and relying on information technology, for example for communication, entertainment, or work (European Commission, 2020; Statistics Netherlands, 2021). This increased reliance on information technology also increases the risk of cybercrime victimization. In the Netherlands, for example, victimization of online crime has increased by 22% since 2012 (Akkermans et al., 2022). In 2021, 28% of the small and medium-size enterprises (SMEs) in the European Union reported cybercrime victimization (European Commission, 2022). In recent years, ransomware has emerged as one of the most prominent cyberthreats for organizations (Europol, 2021; Federal Bureau of Investigation, 2021; Theocharidou et al., 2021). Ransomware is a type of malicious software that makes data inaccessible to the user, typically through encryption, until the victim pays a ransom (Al-rimy et al., 2018; National Crime Agency, 2020). While financial costs are already substantial as a result of ransom payments, loss of turnover or recovery efforts, victimization can simultaneously lead to other damages such as loss of data, reputational damage, or bankruptcy (Brennenraedts et al., 2022; Connolly and Borrion, 2022; Knebel et al., 2021).

Especially vulnerable in this regard are small and medium-sized enterprises (SMEs). In the EU, SMEs make up 99.8% of all enterprises in the business economy (Eurostat, 2022) and many rely on IT and store sensitive data (European Commission, 2022; Veenstra et al., 2015). However, entrepreneurs do not always take sufficient measures to protect against cyber incidents such as ransomware (Moneva and Leukfeldt, 2023; Notté et al., 2019; Rohn et al., 2016; Statistics Netherlands, 2022). For example, the majority of the entrepreneurs do not log and monitor network or user activity and allow employees to use their own devices (Moneva and Leukfeldt, 2023; Notté et al., 2019). Moreover, entrepreneurs often do not consider it very likely that they will be victimized (Bekkers et al., 2023; Brennenraedts et al., 2022; Misana-ter Huurne et al., 2020). Combined, this makes them vulnerable to ransomware victimization.

While a few scientific studies have been conducted on victimization of ransomware among consumers and organizations (e.g. Ortloff, 2021; Simoiu et al., 2019; Voce and Morgan, 2021), little is currently known about how SMEs respond to victimization. For example, SME owners may be more susceptible to paying the ransom demand when they are victimized compared to individuals who do not own or work for an SME, according to an Australian study (Voce and Morgan, 2021). However, it is unclear whether the same applies to SMEs from other countries and whether similar factors contribute to the decision to pay the ransom. Such insights are important to gain a better understanding of the scope and severity of the problem. Furthermore, it can create a better understanding of the decision-making of victims when it comes to ransom payments and what makes them vulnerable to extortion. This can help determine how ransomware attacks aimed at SMEs can be mitigated.

The goal of the current study is to understand decision-making of Dutch SMEs regarding ransom payments; and, in particular, to determine how three dimensions based on previous research (Voce and Morgan, 2021) – the affordability of the ransom, advice from others and having back-ups - affect the decision to pay a ransom. This paper is structured as follows. The next section provides an overview of the literature related to the prevalence of ransomware victimization and ransom payment decision-making, as well as the research question for the current study. This is followed by a description of the research design and the results. In the last section, the main findings, implications and limitations are discussed.

2. LITERATURE REVIEW

2.1. Prevalence of ransomware victimization

The prevalence of ransomware and other types of cybercrime is difficult to determine on the basis of police reports because cybercrimes are generally underreported (van de Weijer et al., 2019). Underreporting may occur because victims do no think the incident is serious enough to report, are able to deal with the incident internally or with the help of an organization other than the police, or because there is a lack of trust in the police when it comes to combatting cybercrime (Cybbar and Center for the Study of Democracy, 2023; Van de Weijer et al., 2020; Veenstra et al., 2015; Wanamaker, 2019). Police report rates are particularly low when ransomware victimization is concerned. A Dutch study found that only 5.7% of consumers and 16.7% of companies that fell victim to ransomware attacks reported the incident to the police (Van de Weijer et al., 2020). At the same time, multiple studies have found that victims of ransomware are more inclined to turn to other parties for help, such as friends or family, external consultants, a cybersecurity company or a financial institution (Connolly and Borrion, 2022; Simoiu et al., 2019; Voce and Morgan, 2022; Yilmaz et al., 2022).

While it is difficult to determine the prevalence of ransomware victimization on the basis of police records, some insight is provided by self-report studies. Reports from cybersecurity companies, based on non-representative survey data among IT professionals, demonstrate uncertainty behind ransomware victimization figures, indicating that between 34% and 71% of organizations (including, but not limited to SMEs) around the world have been victimized (ActualTech Media, 2022; CyberEdge Group, 2022; Sophos, 2021). Furthermore, a few empirical studies have focused on the prevalence of ransomware victimization among SMEs. An Australian study among 2,166 SME owners found that owners had a statistically significant higher prevalence of ransomware victimization in their lifetime (8.7%, n = 187) and last year (4.8%, n = 103) compared to SME employees and non-owners/employees (Voce and Morgan, 2021).[1] A Dutch study found that 5.5% among a sample of 529 SME entrepreneurs were victimized by ransomware in 2019 and 3.2% among a sample of 768 SME entrepreneurs were victimized by ransomware in 2021 (Van de Weijer and Leukfeldt, 2023). On a European level, 4% of 12,863 surveyed SMEs in the EU were victimized by ransomware in the last year (European Commission, 2022). Summarized, empirical studies indicate that the prevalence of ransomware victimization among SMEs over a one year-period is between 3 and 6%.

Differences in the prevalence rates between cybersecurity reports and empirical studies can be attributed to various factors. Firstly, sample sizes vary between studies and are not always representative, which may have affected the results. Moreover, some cybersecurity reports are not exclusively aimed at SMEs, but also at large organizations. Secondly, the way victimization has been measured may have influenced the prevalence rates as definitions of ransomware used in the questionnaires vary between studies. Thirdly, findings from cybersecurity reports may be biased because of the commercial nature of the companies (i.e. creating a sense of urgency to sell products or services). All in all, although previous research shows that ransomware victimization is prevalent among organizations, it is unclear to what extent, and illustrates that more insight is needed into this phenomenon.

2.2. Ransom payment decision-making

Ransomware can be characterized as a complex crime, requiring different actions from both perpetrators and victims. For example, prior to execution of the ransomware, perpetrators need to set up the infrastructure, gain access to a victim's system, create persistence and expand access (Matthijsse et al., 2023). Once the data is encrypted and the victim is confronted with the ransom note, it is up to the victim to decide whether or not to pay the ransom. An empirical study based on 353 police reports filed by victimized individuals and organizations in the Netherlands demonstrates that 21% paid the ransom (Meurs et al., 2022). Another empirical study specifically among SMEs indicates that 32.2% of SME owners paid the ransom. Moreover, the authors found a statistically significant relationship between being a SME owner and payment of the ransom (Voce and Morgan, 2021).

Previous research has examined what factors may affect the decision to pay the ransom. Some studies have looked at characteristics of ransom notes that might influence decision-making concerning payment. Hadlington (2017) analyzed 76 splash screens (i.e. ransom notes), examining the use of three psychological mechanisms used in social engineering – scarcity, authority, and liking[2] - that attackers may use to influence the victim (see also Cialdini, 2006). A sense of scarcity is created by a countdown timer, a message stating that the data can only be decrypted by the attackers, or other threats such as deletion or leaking of data after expiration of the deadline. Scarcity can create a sense of urgency forcing victims into quick decision-making. In addition, splash screens containing clear, detailed information, customer service or the use of official trademarks, logos (e.g. a law enforcement logo) or imagery may create a sense of authority and make victims feel more confident that they will get their files back after payment. Lastly, a splash screen can include humorous or conversational text to induce the victim to like the attacker and comply with payment (Hadlington, 2017).

While the impact of the mechanisms on payment decision-making was not tested in the study by Hadlington (2017), other experimental studies have tested this. Arief et al. (2020) found no clear relationship between the design of a ransomware screen (either a text-based splash screen, a screen with a countdown timer, and a screen with a more advanced user interface) and the likelihood of paying. Respondents did indicate that an authoritarian tone (e.g. pretense of law enforcement), typos, the mention of Bitcoin, complicated instructions, and no clear way of contacting the attackers would discourage them from paying the ransom (Arief et al., 2020). Yilmaz et al. (2021) also researched whether a splash screen design affects the individual's likelihood of paying the ransom, as well as the likelihood of reporting the incident. Respondents (*n* = 538) were presented with one type of mock-up splash screen (either a text, a graphical user interface, or a graphical user interface with a timer) in a randomized controlled experiment. About 5% of the respondents indicated that they would pay the ransom. No statistically significant differences were found among the experimental groups in terms of the likelihood of paying (Yilmaz et al., 2021). The results from both experimental studies indicate that other factors than the design of the ransom note might play a role in influencing payment decision-making.

Other studies have looked at the reasoning and characteristics of victims in relation to ransom payments. Payment decision-making is often based on a cost-benefit analysis and victims can have multiple motives for (not) paying (Connolly and Borrion, 2022). Based on the literature, reasons why individuals and organizations pay include: not being able to restore data from back-ups, not wanting to lose data, following received advice to pay, the downtime being too long, the threat of bankruptcy, fear of incrimination by data protection authorities, the possibility of stolen data being leaked or sold online if not paying, the belief that they will get access to data back after paying, the ability to afford the ransom, and a lack of computer knowledge (Connolly and Borrion, 2022; Matthijsse et al., 2023; Simoiu et al., 2019; Voce and Morgan, 2021). In addition, a police report-based study showed that the likelihood the ransom is paid is significantly related to the ransom amount requested after negotiations, the number of days of negotiating, data exfiltration, being blackmailed (e.g. the attackers contacting employees or customers) and the ability to recover through a back-up (Meurs et al., 2022).

When it comes to SMEs specifically, Voce and Morgan (2021) found that a higher proportion of SME owners paid the ransom because of the advice they received and because they could afford the ransom compared to non-SME owners or employees, although these differences are not statistically significant, possibly due to the sample size. The literature contradicts on the role insurance may play. While a study based on expert interviews found that victims paid the ransom because they are insured (Matthijsse et al., 2023), victims in a survey-based study indicated that they paid the ransom because they did not have insurance, or that they did not pay because they did have insurance (Voce and Morgan, 2021). A statistically significant higher proportion of SMEs did not pay because they had insurance compared to SME employees and non-SME owners (Voce and Morgan, 2021). While the studies provide no further details, this contradiction could be explained by the fact that uninsured victims may find that paying the ransom is a more viable option than bearing the financial costs that are often associated with ransomware victimization and that they are not insured for, such as recovery costs or loss of revenue due to halted business operations (Brennenraedts et al., 2022; Connolly and Borrion, 2022; Knebel et al., 2021). On the other hand, the ransom payment is often reimbursed to insured victims, depending on the type of coverage, which might encourage and facilitate ransom payments (Mott et al., 2023).

Based on the literature, reasons for individuals and organizations not to pay include: being able to recover through back-ups or another way; not being able to afford the ransom amount; following advice to not pay; believing the threat is a scam; avoiding further extortion; believing that it is unethical to pay criminals or to facilitate crime; and being uncertain about the outcome as cybercriminals might keep a copy of the stolen data to sell or leak afterwards (Connolly and Borrion, 2022; Matthijsse et al., 2023; Voce and Morgan, 2021, 2022; Yilmaz et al., 2021). When it comes to SMEs, a study found that the most common reasons for not paying were: advice they had received, not believing the ransom demands were genuine and the availability of back-ups (Voce and Morgan, 2021). Moreover, although a statistically significant difference was not found, a higher proportion of SME owners believed their data would be leaked or sold irrespective of whether they paid or not (Voce and Morgan, 2021).

2.3. Aim of current study

Despite the increasing number of studies conducted on ransomware victimization, a knowledge gap still remains. Firstly, more insight is needed into payment decision-making after a ransomware attack. Research shows that ransom payments sustain the ransomware ecosystem as payments are used to attack and extort new victims (Matthijsse et al., 2023). However, little is currently known about the factors influencing the likelihood of payment. Secondly, more empirical research is needed on ransomware incidents among SMEs. Few studies have focused on SMEs, despite the fact that they are seemingly at a high risk. It is important to obtain a clear picture of how SMEs respond to ransomware victimization and what affects their decision-making. This can in turn provide insight into how attacks can be mitigated.

To address this gap in the literature, this study focuses on ransomware victimization among SMEs in the Netherlands, and poses the following research question:

> Q1: To what extent does the affordability of the ransom, received advice on whether to pay, and having a back-up affect the likelihood of paying a ransom among Dutch SMEs?

3. DATA AND METHOD

3.1.Sample

To answer the research question, we aimed to recruit a sample of individuals who were aware of the ransomware incidents their SME is facing, and who were in a position to decide whether or not to pay the ransom. Based on the European Commission recommendation, SMEs were defined as "enterprises which employ fewer than 250 persons and which have an annual turnover not exceeding EUR 50 million, and/or an annual balance sheet total not exceeding EUR 43 million." (Article 2, Recommendation 2003/361/EC). This includes micro enterprises with less than 10 employees and an annual turnover that does not exceed €2 million, small enterprises with between 10 and 49 employees and an annual turnover that does not exceed €10 million, and medium enterprises with between 50 and 250 employees and an annual turnover not exceeding €43 million.

We relied on two panels from the research firm I&O Research to administer a survey to a sample of owners or managers of SMEs in the Netherlands.[3] I&O Research employs a consumer panel of 35,000 Dutch citizens that are selected through random sampling (e.g., from residence registers). Panelists receive points for each completed survey, which they can redeem for a gift card or a donation to a charity (I&O Research, n.d.-a). In addition, they employ a panel of 4.500 Dutch entrepreneurs (I&O Research, n.d.-b). A total of 1.603 panelists from the consumer and entrepreneurial panel were invited to participate, of which 568 (35.4%) responded between January 31 and February 14, 2022. To ensure that potential respondents belonged to the target group, a filter question was included at the beginning of the questionnaire, asking respondents whether they identified as entrepreneurs with staff. Furthermore, they were required to indicate the size of the company to ensure SME status. A total of 111 respondents were consequently filtered out or did not complete the questionnaire. Another 12 respondents were excluded from the analyses because they rushed through the questionnaire and were considered *speeders*. Based on the entire distribution of the response time in minutes (*M* = 203; *SD* = 1108; *Mdn* = 6), we defined as speeders those respondents with a response time less than 3 minutes. No upper threshold was applied, as the distribution suggests that some respondents took a break and completed the questionnaire at a later time. This resulted in a sample of 445 respondents (response rate: 27.7%).

Initially, micro enterprises were underrepresented in the sample. To make the sample more reflective of the larger population, observations were weighted according to company size[4] to make the sample representative of the population of SMEs in the Netherlands in the first quarter of 2022 (StatLine, 2022). This was done using a cell-weighting procedure, where weights were determined for each cell in the distribution of company size by dividing the population proportion by the sample proportion. In the weighted sample, most organizations were micro enterprises with 1 to 9 employees (96.6%), some were small enterprises with 10 to 49 employees (2.7%), and the remaining were medium enterprises with 50 to 250 employees (0.7%).[5] Organizations had been in operation for 23.9 years on average at the time of the survey. Of the respondents, 7.4% was ever victimized by ransomware. None of the victims were victimized in the last year. The characteristics of the sampled enterprises before and after applying the weights are included in Table 2. This table also illustrates how the weighting affected the distribution of each variable that was included in the analysis.

3.2. Instrument

To collect the data, an online questionnaire in Dutch inspired by the Home Office's Cyber Security Breaches Survey (Johns, 2020) was administered, consisting of four blocks of items. The first part of the questionnaire contained questions about the characteristics of the organization such as the size of the company and the activities of employees. In the second part, respondents were asked about the organizations' attitude towards cybersecurity. In the third part, questions were asked about actual ransomware victimization and hypothetical scenarios (vignettes) relating to ransom payment decision-making. Lastly, respondents were asked about the cybersecurity measures and procedures that were in place. The focus in this study lies on the first and third block.

3.3. Measures

3.3.1. Dependent and independent variables

A vignette experiment was used to examine the factors that determine whether a ransom is paid by victims. A vignette is "a short, carefully constructed description of a person, object, or situation, representing a systematic combination of characteristics" (Atzmüller and Steiner, 2010, p. 128), to elicit attitudes, decisions or judgments from participants (Aguinis and Bradley, 2014; Atzmüller and Steiner, 2010). As a vignette experiment involves a hypothetical scenario, it is a useful research method for sensitive subject matters (such as ransomware victimization) where experimental research is less appropriate because of ethical concerns, while still exercising control over the included variables that might influence decision-making behavior (Aguinis and Bradley, 2014). Furthermore, it enhances realism and validity and reduces social desirability bias compared to direct survey questions (Wason et al., 2002).

3.3.1.1. Power

Prior to the data collection, a power analysis (Cohen, 1988) was conducted to determine the necessary sample size to compare groups and observe statistical differences with sufficient confidence (*power* = 0.8; *alpha* = 0.05). A two-sample t-test power calculation indicated that the optimal sample size would be at least 26 for each comparison group to observe large effect sizes (*Cohen's d* = 0.8); at least 64 to observe medium effect sizes (*Cohen's d* = 0.5); and at least 394 to observe small effect sizes (*Cohen's d* = 0.2). Considering an expected sample of ~550 as estimated by the panel agency prior to the data collection, the vignette could accommodate four manipulations (16 groups of *n* = 34 participants), three manipulations (8 groups of *n* = 69 participants), and none, respectively. In addition, a linear regression power analysis indicated that the optimal sample size based on three predictors would be at least 36 to observe large effect sizes (*Cohen's f squared* = 0.35); at least 77 to observe medium effect sizes (*Cohen's f squared* = 0.15); and at least 550 to observe small effect sizes (*Cohen's f squared* = 0.02).

3.3.1.2. Vignette

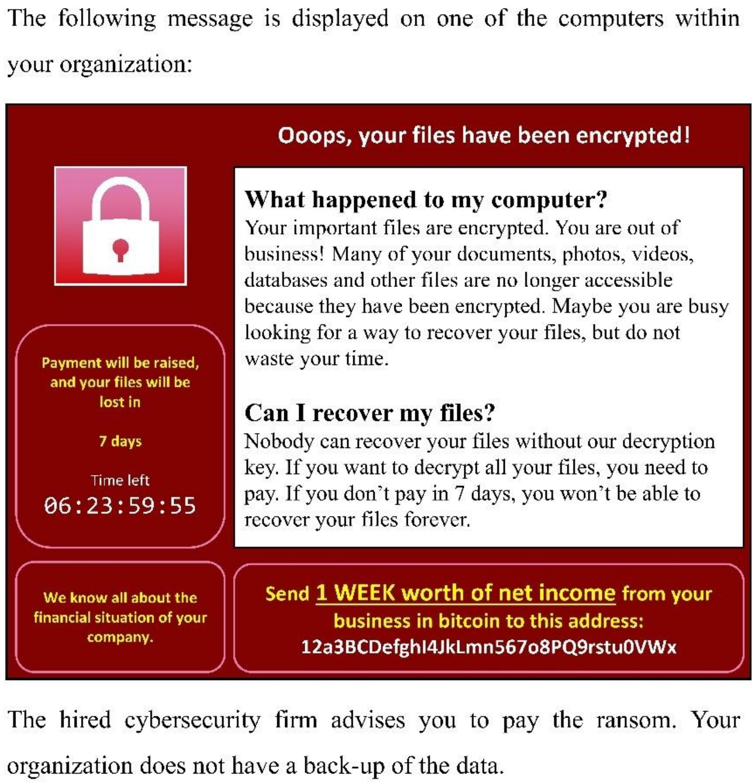
Based on the power analysis and considering an expected sample of ~550, three factors with two variations each were included in the vignette experiment, thus employing a 2 x 2 x 2 design resulting in 8 different vignettes. The factors were based on previous research stating that the decision of SME owners to pay a ransom inter alia depends on the affordability of the ransom, the advice they received whether to pay, and if they had a back-up (Voce and Morgan, 2021). Following a between-subjects design to allow for comparisons between respondents (Atzmüller and Steiner, 2010), participants were randomly assigned to one of eight groups of roughly the same size. Each group was presented with one vignette with a different combination of factor variations. The distribution of vignettes across respondents is included in Table 1.

Table 1 Distribution of vignettes across respondents (weighted sample)

Group	Vignette			Distribution		Likelihood ransom paid	
	Ransom amount (in time worth of net income)	**Advice to pay**	**Back-up**	**N**	**%**	**Mean**	**SD**
1	1 week	Yes	Yes	62	14.0%	.78	1.65
2	1 week	Yes	No	46	10.4%	2.72	3.28
3	1 week	No	Yes	47	10.5%	.64	1.95
4	1 week	No	No	67	15.0%	1.70	2.57
5	3 months	Yes	Yes	57	12.8%	.85	1.76
6	3 months	Yes	No	54	12.2%	2.14	2.97
7	3 months	No	Yes	51	11.5%	.16	.48
8	3 months	No	No	60	13.6%	1.73	2.90

All respondents were asked to imagine the hypothetical situation that their organization was victimized by ransomware and they were tasked with the responsibility to decide whether or not to pay the ransom. They were then shown a ransom note, based on the WannaCry ransom note from 2017 (see Figure 1 as example).[6] The first factor included in the vignette concerned the affordability of the ransom demand, which varied between 1 week's worth of net income from their business in bitcoin and 3 months worth of net income from their business in bitcoin. These thresholds were based on the researchers' experience of what could be considered a low or high financial impact on SMEs. The second factor concerned advice on whether to pay or not, varying between 'the hired cybersecurity firm advises you to not pay the ransom' and 'the hired cybersecurity firm advises you to pay the ransom'. The third factor concerned the existence of a back-up, varying between 'your organization has a back-up of the data' and 'your organization does not have a back-up of the data'. These factors were used as independent variables in the analyses. For easy interpretation of the results, the variables were recoded so that value 0 reflects the least likely and value 1 the more likely scenario in which potential victims would pay the ransom, resulting in the dichotomous variables affordability of the ransom demand (0 = 3 months worth of net income from their business in bitcoin, 1 = 1 week's worth of net income from their business in bitcoin), being advised whether or not to pay (0 = advised to not pay the ransom, 1 = advised to pay the ransom), and the existence of a back-up (0 = Back-up of the data, 1 = No back-up of the data).

After being presented with the vignette, respondents were asked to report the likelihood that they would pay the ransom from not likely at all (0%) to very likely (100%). This variable is measured from 0 to 10 (0 = 0%, 1 = 10%, 2 = 20% etc.) and was used in the analysis as dependent variable.



The following message is displayed on one of the computers within your organization:

Ooops, your files have been encrypted!

What happened to my computer?
Your important files are encrypted. You are out of business! Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time.

Can I recover my files?
Nobody can recover your files without our decryption key. If you want to decrypt all your files, you need to pay. If you don’t pay in 7 days, you won’t be able to recover your files forever.

Payment will be raised, and your files will be lost in

7 days

Time left
06:23:59:55

We know all about the financial situation of your company.

Send 1 WEEK worth of net income from your business in bitcoin to this address:
12a3BCDefghI4JkLmn567o8PQ9rstu0VWx

The hired cybersecurity firm advises you to pay the ransom. Your organization does not have a back-up of the data.

Figure 1. Example of vignette (translated from Dutch)

3.3.2. Control variables

The size of the organization, the number of years the organization has been in operation, having insurance and previous ransomware victimization were included in the analysis as control variables; these factors may influence to what extent organizations are able to afford the ransom, what a cybersecurity company advises them in terms of payment and whether they have a back-up, as well as the decision whether or not to pay a ransom. Both the size of the organization (1 = micro (1-9 employees), 2 = small (10-49 employees), 3 = medium (50-250 employees)) and having insurance (1 = specific cyber security insurance policy, 2 = cyber security as part of wider insurance policy, 3 = no insurance, 4 = don’t know) are categorical variables. Years in operation is a continuous variable, measured in the number of years applicable at the time the survey was filled out (0-101). Lastly, previous victimization was included in the analysis as dichotomous variable (0 = no, 1 = yes). For this variable, the category “don’t know” was recoded as “no” since victims are usually aware that they have been victimized because they are confronted with a ransom note and locked or encrypted data. Descriptive statistics of all variables are included in Table 2.

Table 2 Descriptive statistics of included variables (unweighted and weighted sample) [7]

Variable	Unweighted				Weighted			
	N	%	Mean	SD	N	%	Mean	SD
Likelihood ransom paid	445		1.47	2.60	445		1.34	2.46
Years in operation	442		25.83	21.35	441		23.93	19.78
Size organization	445				445			
Micro	310	69.7%			429	96.6%		
Small	112	25.2%			12	2.7%		
Medium	23	5.2%			3	0.7%		
Insurance	445				445			
Specific cyber security insurance policy	32	7.2%			16	3.7%		
Cyber security as part of wider insurance policy	58	13%			57	12.9%		
No insurance	284	63.8%			295	66.4%		
Don't know	71	16%			75	17%		
Previous victimization (ever)	445				445			
No	403	90.6%			412	92.6%		
Yes	42	9.4%			33	7.4%		
Affordability ransom	445				445			
1 week worth's of net income	222	49.9%			222	50%		
3 months worth of net income	223	50.1%			223	50%		
Advised whether or not to pay	445				445			
Advised to pay	211	47.4%			220	49.4%		
Advised to not pay	234	52.6%			225	50.6%		
Back-up	445				445			
Yes	221	49.7%			217	48.8%		
No	224	50.3%			228	51.2%		

3.4. Analytic strategy

Descriptive statistics were used to answer the first research question. To answer the second research question, we first compared the mean likelihood of the ransom being paid for the different vignette factors. Given that the distribution of the likelihood of the ransom being paid is over-dispersed and positively skewed (*M* = 1.34, *SD* = 2.46, Skewness = 1.83, Kurtosis = 2.24) as indicated by a Kolmogorov-Smirnov test (D(445) = .384, p = <.001) as well as visual inspection of the histogram and plots, the assumption of normal distribution was violated. As the variable was positively skewed even after attempts to transform the data[8], non-parametric Mann-Whitney U tests were used to analyze group differences in the likelihood of paying for the dichotomous variables affordability of the ransom demand, being advised whether or not to pay, and the existence of a back-up. We relied on the implementation of the Mann-Whitney U tests provided in the Sjstats R package (Lüdecke, 2022). For *approximated* mean-ranks and effect sizes, the unweighted Mann-Whitney U tests can be found in Table 1 of the appendix. Since we do not know how to determine what a meaningful effect size would be in this context, we rely on the standard thresholds of Cohen (1988, 1992), where *r* = .10 is a small effect size, *r* = .30 is a medium effect size and *r* = .50 is a large effect size.

Second, since the variance of the likelihood of the ransom being paid was larger than the mean (Variance = 6.047, *M* = 1.34), we conducted a negative binomial regression model (Green, 2021; Hilbe, 2011). The model that was used to explain the variance in the likelihood of the ransom being paid included the vignette factors affordability of the ransom demand, being advised whether or not to pay, and the existence of a back-up as predictors. Furthermore, the size of the organization, years in operation, having insurance, and previous victimization were included in the model as control variables. Since the size of the organization and having insurance were categorical variables, these were included as dummy variables in the model, with the category 'micro' and 'not having insurance' as reference categories. The analyses were conducted in IBM SPSS Statistics 28.0 (IBM, 2021), and R version 4.3.1 (R Core Team, 2023) and RStudio version 2023.06.2 (RStudio Team, 2020).

4. RESULTS

All respondents were asked to imagine the hypothetical situation in which their organization was victimized by ransomware. They were then shown a vignette that included factors relating to the affordability of the ransom, being advised whether or not to pay, and whether they had a back-up, and were then asked to report the likelihood of the ransom being paid. On average, respondents in the weighted sample considered the likelihood that they would pay the ransom to be low (*M* = 1.34; *SD* = 2.46).

Mann-Whitney U tests were conducted to analyze group differences in the weighted sample in the likelihood of the ransom being paid for the vignettes (Table 3).[9] The Mann-Whitney U test for the affordability of the ransom was found to be statistically non-significant (*est* = .013; *p* = .629). No statistical difference was found with regard to the likelihood of the ransom being paid between participants who were demanded to pay 1 week's worth of net income in Bitcoin and respondents who were required to pay 3 months worth of net income in Bitcoin. The test for being advised whether to pay was also found to be statistically non-significant (*est* = .038; p = .146). No statistical difference was found with regard to the likelihood of the ransom being paid between participants that were advised by a cybersecurity company to pay the ransom, and participants that were advised to not pay the ransom. The test for having a back-up was found to be statistically significant (*est* = .129; *p* < .001). Participants that did not have a back-up reported a higher likelihood of the ransom being paid compared to participants that did have a back-up.

Table 3 Weighted Mann-Whitney U tests comparing the likelihood of the ransom being paid with the affordability of the ransom, being advised by a cybersecurity company to pay, and having a back-up

Vignette factors	**X²**	**Estimate**	***p***
Affordability ransom	.484	.013	.629
Advised to pay	1.457	.038	.146
Back-up	5.139	.129	.000***

Notes: N=445
*p< .05, **p< .01, ***<.001

Next, negative binomial regression was conducted to determine whether the affordability of the ransom, being advised by a cybersecurity company to pay, and having a back-up were significantly related to the likelihood of the ransom being paid in the weighted sample.[10] The regression model included the predictors affordability of the ransom, being advised whether to pay or not and having a back-up. The size of the organization, years in operation, having insurance, and previous victimization were added to the model as control variables. As shown in table 4, the affordability of the ransom did not significantly predict the likelihood of the ransom being paid (*est* = .241, *z* = 1.125, p = .260). Being advised by a cybersecurity company to pay was a significant predictor of the likelihood of the ransom being paid (*est* = .519, *z* = 2.381, *p* = .017). Being advised by a cybersecurity company to pay, increased the likelihood of paying by .519. Having a back-up also significantly predicted the likelihood of the ransom being paid (*est* = 1.321, *z* = 6.071, *p* <.001). Not having a back-up increased the likelihood of paying by 1.321.

Table 4 Weighted negative binomial regression estimates of the likelihood of the ransom being paid

Variable	**Estimate**	**S.E.**	**z**	***p***	***sig.***
(Intercept)	-.891	.278	-3.200	.001	**
Vignette factors					
Affordability ransom (0-1)	.241	.215	1.125	.260	
Advised to pay (0-1)	.519	.218	2.381	.017	*
Back-up (0-1)	1.321	.218	6.071	.000	***
Control variables					
Years in operation (0-101)	-.003	.006	-.480	.631	
Micro size organization (0-1)	REF				
Small size organization (0-1)	.345	.649	.533	.594	
Medium size organization (0-1)	.971	1.192	.815	.415	
Insurance specific cyber policy (0-1)	-.105	.574	-.182	.855	
Insurance wider policy (0-1)	-.046	.330	-.140	.889	
Insurance no (0-1)	REF				
Insurance don't know (0-1)	.088	.288	.305	.760	
Previous victimization (ever) (0-1)	-.450	.430	-1.047	.295	
Log likelihood	-601.3606				
AIC	1226.7				
BIC	1275.8				

Notes: N=442
*p< .05, **p< .01, ***<.001

5. DISCUSSION

Ransomware is currently one of the most prominent cyberthreats for organizations (Europol, 2021; Federal Bureau of Investigation, 2021; Theocharidou et al., 2021). Small- and medium-sized enterprises seem to be particularly vulnerable to victimization and more likely to pay the ransom (Voce and Morgan, 2021). However, little is currently known about ransomware victimization among SMEs and how they respond to victimization. The aim of this study was to gain insight into the factors relating to the decision to pay a ransom. For this purpose, a survey with a vignette experiment was conducted among 445 owners or managers of SMEs in the Netherlands, to research the extent to which the affordability of the ransom, received advice on whether to pay or not, and having a back-up affect the likelihood of paying a ransom.

The findings show that the likelihood of paying was low. Mann-Whitney U tests show there are no statistical differences in the likelihood of paying between participants who were demanded to pay 1 week's worth of net income in Bitcoin and respondents who were required to pay 3 months worth of net income in Bitcoin. In addition, no statistically significant difference was found between participants that were advised by a cybersecurity company to pay the ransom, and participants that were advised to not pay the ransom. However, having a back-up was found to be statistically significant. Participants that did not have a back-up of the encrypted data, reported a higher likelihood of the ransom being paid compared to participants that did have a back-up. In addition, negative binomial regression was conducted to determine whether these three factors were significantly related to the likelihood of the ransom being paid, while controlling for the size of the organization, years in operation, having insurance, and previous victimization. The results show that the affordability of the ransom demand did not significantly predict the likelihood of the ransom being paid. Contrary to the outcome of the Mann-Whitney U Test, being advised by a cybersecurity company whether or not to pay was a significant predictor in the regression model. Furthermore, having a back-up was a significant predictor. Being advised by a cybersecurity company to pay and having no back-up significantly increased the likelihood of the ransom being paid.

Similar to what was found in the literature (Voce and Morgan, 2021), being advised to pay and not having a back-up increases the likelihood of the ransom being paid among SMEs. However, whereas previous work showed that the decision to pay the ransom is related to whether SMEs can afford the ransom demand (Voce and Morgan, 2021), in this study the affordability of the ransom demand was not significantly related to the likelihood of the ransom being paid. On the one hand, this finding may suggest that the decision to pay a ransom is less of a rational economic process based on the direct costs of the ransom payment than might be expected. It is conceivable that being advised to pay and not having a back-up, or other factors not included in this study, play a more decisive role in the decision to pay the ransom than the affordability of the ransom demand. On the other hand, this finding could also be the result of the way the variable was measured in the vignette experiment. The findings indicate that respondents were generally not inclined to pay and needed to be convinced to do so. For the vignette, we tried to come up with numbers that reflected a low and high ransom amount, 1 week's worth of net income versus 3 months worth of net income in Bitcoin respectively - but it is conceivable that the high ransom did not reflect an amount that was sufficiently high enough to convince people to pay.

All in all, the current study has created a better understanding of the factors that make Dutch SMEs vulnerable to extortion and that influence the decision to pay the ransom. This can help the development of measures to mitigate ransomware attacks aimed at SMEs, or could provide a starting point for the development of an intervention to reduce ransom payments. For one, the findings illustrate the importance of (external) back-ups, which can enable organizations to recover from a ransomware incident without paying the ransom, as already discussed in previous research (e.g. Brennenraedts et al., 2022; Connolly and Borrion, 2022; Dargahi et al., 2019; Matthijsse et al., 2023; Meurs et al., 2022). However, as offenders adapt and come up with new extortion methods to ensure the victim will pay, such threats to leak data or threats of GDPR fines (Connolly and Borrion, 2022; Matthijsse et al., 2023), back-ups might not be sufficient. This development in the modus operandi might call for measures not just aimed at the prevention or mitigation of attacks, but also at discouraging ransom payments. As findings show that the advice victims receive from cybersecurity companies influences ransom payment decision-making, these organizations may play an important role in discouraging ransom payments in the future.

Despite the contributions this study offers, it also has some limitations. Firstly, the sample is not representative of all SMEs in the Netherlands, which may affect external validity. Data was weighted using the only available company characteristic in the survey which was company size. However, the sample is not representative when it comes to other characteristics such as turnover or business sector. As a consequence, the results cannot be generalized to the entire population of SMEs in the Netherlands. Furthermore, as the weight adjustments were considerable given the underrepresentation of micro companies, this may have influenced the precision of the estimates. While the Mann-Whitney U test for the unweighted sample showed a statistically significant relationship between the likelihood of the ransom being paid and being advised to pay (similar to the regression model), this was not the case in the Mann-Whitney U test for the weighted sample. However, the other Mann-Whitney U tests and the negative binomial regression yielded similar results for the weighted and unweighted data.

Secondly, the ransom payment decision-making was explored using a vignette study. Prior to data collection, a power analysis (Cohen, 1988) was conducted to determine the number of manipulations the vignette could accommodate. Since the sample size (445) was smaller than the initial estimates

(550), our ability to detect medium effect sizes was also lower than expected. However, given the statistical significance of our results, we do not believe that the sample size had a significant impact.

Thirdly, to be able to detect medium effect sizes with enough confidence, we had to limit the number of factors included in the vignette to three. However, other factors not explored in this study may play a role in the decision whether or not to pay a ransom, such as the credibility of the attackers, the frequency of back-ups, the value or sensitivity of the encrypted data, the downtime being too long, the threat of data being leaked or sold online, or believing that it is unethical to pay criminals (e.g. Connolly and Borrion, 2022; Matthijsse et al., 2023; Voce and Morgan, 2021). Future research could look at other factors that may influence the decision to pay a ransom, especially given that the modus operandi of ransomware is evolving and double or triple extortion methods such as the threatening to leak data have become more commonplace (Matthijsse et al., 2023).

Fourthly, the average likelihood of paying in the hypothetical scenario is low, while previous research points towards a higher payment rate among individuals and organizations (Meurs et al., 2022; Voce and Morgan, 2021). This begs the question to what extent the decision to pay the ransom in the vignette experiment approximates decision-making behavior in an actual ransomware attack. A vignette experiment was used as it has been proposed as a useful method for research into decision-making related to potentially sensitive topics where experimental research is less appropriate (Aguinis and Bradley, 2014) and a good alternative for direct survey questions, enhancing realism and validity (Wason et al., 2002). Overall, vignettes seem to be an appropriate method for researching a sensitive subject such as ransomware, where victims might be less willing to report that they were victimized or extorted into paying a ransom. However, in order for vignettes to work, they need to be as realistic as possible (Aguinis and Bradley, 2014; Baguley et al., 2022), because unrealistic scenarios merely illustrate what behavior or outcomes *can* occur, but not necessarily what *will* occur in a real situation (Aguinis and Bradley, 2014). In an attempt to increase both the level of immersion and the realism of the vignette, respondents were presented with an image-based vignette: a ransom note modelled after an existing ransom note used by a ransomware group in the past. As a result, the vignette more closely resembled experiences of ransomware victimization in a natural setting, thus eliciting more valid responses (Aguinis and Bradley, 2014). However, there is a possibility that the vignette still did not fully immerse respondents, or that they felt the need to give a socially desirable answer. In this regard, the respondents could have been influenced by the recommendation of the Dutch government and police to never pay the ransom. Moreover, ransomware victimization is a high-stake scenario, which is difficult to replicate in a vignette experiment (Aguinis and Bradley, 2014). While respondents got an impression of the stakes at play (such as ransom costs or imminent data loss), other stakes that can play a role in payment decision-making, such as the downtime of the company, may not have played a prominent role in the minds of the respondents when looking at the vignette. In addition, the stress induced by a ransomware incident was absent. As a result, it is conceivable that even though a ransom note was used, the vignette did not create the same context as in 'real life' and thus did not produce the same response as it would have in a natural setting (Aguinis and Bradley, 2014). Thus, the current study measured intended decision-making under specific circumstances, and may not be generalizable to victims of ransomware. While previous research into ransomware involved self-report surveys and experiments with ransom notes (e.g. Arief et al., 2020; Voce and Morgan, 2021; Yilmaz et al., 2021), to our knowledge, the current study is the first to explore the use of a vignette experiment to study decision-making in connection with ransomware victimization. Although the current study cannot contribute to assessing the reliability of vignette experiments in the context of ransomware victimization, it may be a promising method to assess decision-making behavior without directly studying victimization. Future research could be aimed at improving the realism and immersion of the vignette to elicit more valid responses, as well as assess the validity and reliability of vignette experiments in the study of ransomware, for example through comparison with the decision-making of victims.

REFERENCES

ActualTech Media (2022) 2022 Ransomware Survey Results. Infographic. North Charleston: ActualTech

Media.

Aguinis H and Bradley KJ (2014) Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods* 17(4): 351–371. https://doi.org/10.1177/1094428114547952

Akkermans M, Kloosterman R, Moons E, et al. (2022) Veiligheidsmonitor 2021. Report. The Hague: Statistics Netherlands.

Al-rimy BAS, Maarof, MA and Shaid, SZM (2018) Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security* 74: 144–166. https://doi.org/10.1016/j.cose.2018.01.001.

Arief B, Periam A, Cetin O, et al. (2020) Using eyetracker to find ways to mitigate ransomware. In: *Proceedings of the 6th International Conference on Information Systems Security and Privacy*, Valetta, Malta, 25-27 February 2020, pp. 448–456. Portugal: Science and Technology Publications. https://doi.org/10.5220/0008956004480456

Atzmüller C and Steiner PM (2010) Experimental vignette studies in survey research. *Methodology* 6(3): 128–138. https://doi.org/10.1027/1614-2241/a000014

Baguley T, Dunham G and Steer O (2022) Statistical modelling of vignette data in psychology. *British Journal of Psychology* 113: 1143–1163. https://doi.org/10.1111/bjop.12577

Bekkers L, Van 't Hoff-de Goede S, Misana-ter Huurne E, et al. (2023) Protecting Your Business against Ransomware Attacks? Explaining the Motivations of Entrepreneurs to Take Future Protective Measures against Cybercrimes Using an Extended Protection Motivation Theory Model. *Computers & Security* 127: 1-12. https://doi.org/10.1016/j.cose.2023.103099

Brennenraedts R, Van der Vorst T, Kats J, et al. (2022) *Verkenning risicofactoren ransomware-aanvallen*. Report. The Hague: WODC.

Cialdini RB (2006). *The Psychology of Persuasion*. Harper Business.

Cohen J (1988) *Statistical Power Analysis for the Behavioral Sciences*. Hillsdale: Lawrence Erlbaum Associates.

Cohen J (1992) A Power Primer. *Psychological Bulletin* 112(1): 155–159.

Connolly LY and Borrion H (2022) Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Computers & Security* 119: 1–14. https://doi.org/10.1016/j.cose.2022.102760

Cybbar and Center for the Study of Democracy (2023). Cybercrime against businesses in the EU: Challenges to Reporting. Policy Brief. Cybbar/Sofia: Center for the Study of Democracy.

CyberEdge Group (2022) 2022 Cyberthreat Defense Report. Report. Annapolis: CyberEdge Group.

Dargahi T, Dehghantanha A, Bahrami PN, et al. (2019) A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques* 15(4): 277–305. https://doi.org/10.1007/s11416-019-00338-7

European Commission (2020) Special Eurobarometer 499 – Europeans' attitudes towards cyber security. Report. European Commission. https://doi.org/10.2837/672023

European Commission (2022) Flash Eurobarometer 496 – SMEs and cybercrime. Report. European Commission. https://doi.org/10.2837/89101

Europol (2021) Internet Organised Crime Threat Assessment (IOCTA) 2021. Report. Luxembourg: Publications Office of the European Union. https://doi.org/10.2813/113799

Eurostat (2022) *Number of persons employed by enterprise size class, 2019. Available at:* https://ec.europa.eu/eurostat/cache/infographs/sbs_2022/#small (accessed 28 February 2023)

Federal Bureau of Investigation (2021) Internet Crime Report 2021. Report. Internet Crime Complaint Center, Federal Bureau of Investigation.

Grauer K, Kueshner W and Updegrave H (2022) The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime. Report. New York: Chainanalysis.

Green JA (2021) Too many zeros and/or highly skewed? A tutorial on modelling health behaviour as count data with Poisson and negative binomial regression. *Health Psychology and Behavioral Medicine* 9(1): 436–455. https://doi.org/10.1080/21642850.2021.1920416

Hadlington L (2017) Exploring the Psychological Mechanisms used in Ransomware Splash Screens. Report. Leicester: De Montfort University.

Hilbe JM (2011) *Negative Binomial Regression*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511973420

IBM (2021) *IBM SPSS Statistics for Windows, Version 28.0.* IBM.

I&O Research (n.d.-a) I&O Research Panel. Available at: https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/ (accessed 14 april 2023)

I&O Research (n.d.-b) I&O Research Ondernemerspanel. Available at: https://www.ioresearch.nl/onderzoeksmethoden/io-research-ondernemerspanel/ (accessed 14 april 2023)

Johns E (2020) Cyber Security Breaches Survey 2020: Statistical Release. Report. London: Department for Digital, Culture, Media & Sport.

Knebel S, Schultz MD and Seele P (2021) Cyberattacks as “state of exception” reconceptualizing cybersecurity from prevention to surviving and accommodating. *Journal of Information, Communication and Ethics in Society* 20(1): 1–19. https://doi.org/10.1108/JICES-01-2021-0015

Lüdecke, D (2022) *Sjstats: Statistical Functions for Regression Models.*

CRAN. https://doi.org/10.5281/ZENODO.1284472.

Matthijsse SR, Van ’t Hoff-de Goede MS and Leukfeldt ER (2023) Your files have been encrypted: a crime script analysis of ransomware attacks. *Trends in Organized Crime*. Online first. https://doi.org/10.1007/s12117-023-09496-z

Meurs T, Junger M, Tews E, et al. (2022) Ransomware: How attacker’s effort, victim characteristics and context influence ransom requested, payment and financial loss. In: *APWG Symposium on Electronic Crime Research (eCrime),* Virtual event, 30 November – 2 December 2022, pp. 1-13. https://doi.org/10.1109/eCrime57793.2022.10142138.

Misana-ter Huurne E, Van Houten Y, Spithoven R, et al. (2020) Cyberweerbaarheid. Risicobewustzijn en zelfbeschermend gedrag rondom cybercrime onder jongeren en mkb’ers. Report. Apeldoorn: Saxion University of Applied Sciences/The Hague: The Hague University of Applied Sciences

Moneva A and Leukfeldt R (2023) Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures. *Journal of Criminology* 56(4): 416-440. https://doi.org/10.1177/26338076231161842

Mott G, Turner S, Nurse JRC, et al. (2023) Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security* 128: 1-21. https://doi.org/10.1016/j.cose.2023.103162

National Crime Agency (2020) National Strategic Assessment of Serious and Organised Crime. Report. London: National Crime Agency.

Notté RJ, Slot LK, Van ‘t Hoff-de Goede MS, et al. (2019) Cybersecurity in het mkb: nulmeting. Report. The Hague: The Hague University of Applied Sciences.

Ortloff A-M, Vossen M and Tiefenau C (2021) Replicating a study of ransomware in Germany. In: *Proceedings of the 2021 European Symposium on Usable Security*, Karlsruhe, Germany, 11-12 October 2021, pp. 151–164. New York: Association from Computing Machinery. https://doi.org/10.1145/3481357.3481508

R Core Team (2023) *R: A language and environment for statistical computing.* https://www.R-project.org/

Recommendation 2003/361/EC. *Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361

Rohn E, Sabari G and Leshem G (2016) Explaining small business InfoSec posture using social theories. *Information and Computer Security* 24(5): 534–556. https://doi.org/10.1108/ICS-09-2015-0041

RStudio Team (2020) *RStudio: Integrated development environment for R*. http://www.rstudio.com/

Simoiu C, Gates C, Bonneau J, et al. (2019) "I was told to buy a software or lose my computer. I ignored it": A study of ransomware. In: *Proceedings of the 15th USENIX Symposium on Usable Privacy and Security*, Santa Clara, United States, 12-13 August 2019, pp. 155–174. Berkely: USENIX Association.

Sophos (2021) The State of Ransomware 2021. Report. Abingdon: Sophos

StatLine (2022) Bedrijven; bedrijfstak. Available at: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/81589NED/table (accessed 10 January 2023).

Statistics Netherlands (2021) ICT, kennis en economie 2021. Report. The Hague: Statistics Netherlands.

Statistics Netherlands (2022) Cybersecuritymonitor 2021. Report. The Hague: Statistics Netherlands.

Theocharidou M, Malatras A, Lella I., et al. (2021) ENISA Threat Landscape 2021: April 2020 to mid-July

2021. Report. Athens: European Network and Information Security Agency. https://doi.org/10.2824/324797

Van de Weijer SGA, Leukfeldt ER and Van der Zee S (2020) Slachtoffer van online criminaliteit, wat nu? Een onderzoek naar de aangiftebereidheid onder burgers en ondernemers. Report. Den Haag: SDU Uitgevers/Amsterdam: Politie & Wetenschap/Amsterdam: NSCR

Van de Weijer SGA and Leukfeldt R (2023) Cybercriminaliteit tijdens de coronacrisis: Aard, omvang en impact van cyberrisico's voor burgers en het mkb. Report. Amsterdam: NSCR/The Hague: The Hague University of Applied Sciences.

Van de Weijer SGA, Leukfeldt R and Bernasco W (2019) Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16(4): 486–508. https://doi.org/10.1177/1477370818773610

Veenstra S, Zuurveen R and Stol W (2015) Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden-en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland. Report. Leeuwarden: NHL Stenden/Apeldoorn: Politie Academy/Heerlen: Open Universiteit

Voce I and Morgan A (2021) Ransomware victimisation among Australian computer users. *Statistical Bulletin* 35: 1–17.

Voce I and Morgan A (2022) Help-seeking among Australian ransomware victims. *Statistical Bulletin* 38: 1–13. https://doi.org/https://doi.org/10.52922/sb78504

Wanamaker KA (2019) *Profile of Canadian businesses who report cybercrime to police: The 2017 Canadian Survey of Cyber Security and Cybercrime*. Report. Ottawa: Public Safety Canada.

Wason KD, Polonsky MJ and Hyman MR (2002) Designing Vignette Studies in Marketing. *Australasian Marketing Journal* 10(3): 41–58. https://doi.org/10.1016/s1441-3582(02)70157-2

Yilmaz Y, Cetin O, Arief B, et al. (2021) Investigating the impact of ransomware splash screens. *Journal of Information Security and Applications* 61: 1–13. https://doi.org/10.1016/j.jisa.2021.102934

Yilmaz Y, Cetin O, Grigore C, et al. (2022) Personality Types and Ransomware Victimisation. *Digital Threats: Research and Practice* 4(4): 1-25. https://doi.org/10.1145/3568994

APPENDIX

Table 1 Unweighted Mann-Whitney U tests comparing the likelihood of the ransom being paid with the affordability of the ransom, being advised by a cybersecurity company to pay, and having a back-up

Vignette factors	**n**	**Mean rank**	**U**	**z**	***p***	**Sig.**	***r***
Affordability ransom			49371.500	-0.311	.756		.015
3 months worth of net income	223	221.40					
1 week’s worth of net income	222	224.61					
Advised to pay			49538.500	-2.301	.021	*	.109
No	234	211.70					
Yes	211	235.53					
Back-up			42315.500	-6.056	<.001	***	.287
Yes	221	191.47					
No	224	254.10					

Notes: N=445
*p< .05, **p< .01, ***<.001

DECLARATIONS

Conflict of interest

The authors have no competing interests to declare that are relevant to the content of this article.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

FOOTNOTES

[1] The ransomware attack was not necessarily related to the business.

[2] The concept that an individual is more likely to comply with a request if they like the person (Cialdini, 2006; Hadlington, 2017).

[3] Ethical advice for the study was received from the Ethical Advisory Committee of the Hague University of Applied Sciences.

[4] The only available company characteristic.

[5] Definitions of micro, small and medium-sized enterprises are based on EU recommendation 2003/361.

[6] The original WannaCry ransom note featured two different countdowns, one for a raise of the payment and one for permanent loss of files.

[7] Frequencies for some variables in the weighted sample do not equal totals due to rounding as a result of weighting the data.

[8] Using log transformation, square-root transformation, and reciprocal transformation.

[9] Mann-Whitney U tests were also conducted for the unweighted sample (see appendix). This yielded similar results for the affordability of the ransom and having a back-up, but a different result for being advised to pay.

[10] Negative binomial regression was also conducted for the unweighted sample, which yielded similar results.