Computers & Security 127 (2023) 103099

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

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

Luuk Bekkers[a,b,*], Susanne van 't Hoff-de Goede[a], Ellen Misana-ter Huurne[b], Ynze van Houten[b], Remco Spithoven[b], Eric Rutger Leukfeldt[a,c]

[a] *The Hague University of Applied Sciences, Johanna Westerdijkplein 75, 2521 EN, The Hague, the Netherlands*
[b] *Hogeschool Saxion, Spoorstraat 29, 7311 PE, Apeldoorn, the Netherlands*
[c] *Netherlands Institute for the Study of Crime and Law Enforcement, De Boelelaan 1077, 1081 HV, Amsterdam, the Netherlands*

ARTICLE INFO

Article history:
Received 10 June 2022
Revised 3 October 2022
Accepted 10 January 2023
Available online 14 January 2023

Keywords:
Ransomware
Cybercrime victimization
Entrepreneurs
Cyber resilience
Extended protection motivation theory

ABSTRACT

Entrepreneurs are likely to be victims of ransomware. Previous studies have found that entrepreneurs tend to adopt few preventive measures, thereby increasing their chances of victimization. Due to a lack of research, however, not much is known about why entrepreneurs lack self-protective behaviors and how they can be encouraged to change said behaviors. Therefore, the purpose of this study is to explain, by means of an extended model of the Protection Motivation Theory (PMT), the motivation for entrepreneurs using protective measures against ransomware in the future. The data for our study were collected thanks to a questionnaire that was answered by 1,020 Dutch entrepreneurs with up to 250 employees. Our Structural Equation Modelling (SEM) analysis revealed that entrepreneurs are more likely to take preventive measures against ransomware if they perceive the risk of ransomware as severe (perceived severity), if they perceive their company as being vulnerable (perceived vulnerability), if they are concerned about the risks (affective response), and if they think that the people and companies around them expect them to apply preventive measures (subjective norms). However, if entrepreneurs think that they are capable of handling the risk (self-efficacy) and are convinced that their adopted preventive measures are effective (response efficacy), they are less likely to take preventive measures. Furthermore, for entrepreneurs that outsource IT security, the significant effect of perceived vulnerability and subjective norms disappears. The likelihood of entrepreneurs protecting their business against ransomware is thus influenced by a complex interplay of various motivational factors and is partly dependent on the business' characteristics. Based on these findings, we will discuss security professionals' prospects for increasing the cyber resilience of entrepreneurs, thus preventing cybercrime victimization.

1. Introduction

Nowadays, ransomware falls under the heading of most prevalent form of cybercrime for entrepreneurs (i.e. freelancers and the owners of small- and medium-sized enterprises (SMEs) with up to 250 employees) (Johns, 2021; Notté et al., 2019; Veenstra et al., 2015; Sophos, 2022). Ransomware refers to a type of malicious software, i.e. malware, that locks a computer system or prevents users from accessing their data until the victim pays a ransom (Richardson and North, 2017); this is in contrast to other forms of malware that are often aimed at replicating, deleting or overburdening system resources. A worldwide survey among information technology (IT) professionals found that around two thirds of medium-sized organizations were hit by a ransomware attack in 2021, a significant increase compared to 2020 (Sophos, 2022). Almost half of the victims paid the ransom, which amounted to more than 800,000 US dollars on average, and it took companies around a month to recover from the attack. In the case of Dutch entrepreneurs, Notté et al. (2019) report that seventeen percent

[*] Corresponding author.
E-mail addresses: l.m.j.bekkers@hhs.nl (L. Bekkers), m.s.vanthoff-degoede@hhs.nl (S. van 't Hoff-de Goede), e.f.j.misana@saxion.nl (E. Misana-ter Huurne), y.a.vanhouten@saxion.nl (Y. van Houten), r.spithoven@saxion.nl (R. Spithoven), e.r.leukfeldt@hhs.nl (E.R. Leukfeldt).

https://doi.org/10.1016/j.cose.2023.103099

of SMEs have been victimized by ransomware that at some point, resulted in damage in terms of money, time or resources. These statistics indicate that entrepreneurs suffer the long-lasting consequences of ransomware attacks and are likely to be targets of such attacks; perhaps even more so than other groups of individuals, as is now recognized by cybercrime scholars (e.g. Leukfeldt, 2018).

However, to date, little research has focused on this specific group of potential targets, who are generally difficult to reach and recruit for research purposes. Therefore, not much is known about why entrepreneurs are victimized by ransomware relatively often and how future victimization can be prevented. Because taking cybersecurity measures can decrease the likelihood of ransomware victimization, this study focuses on the motivation of entrepreneurs adopting self-protective behaviors in the future. Self-protective behaviors refer to those actions or behaviors that people perform to protect themselves from risks, danger or their consequences (Spithoven, 2020; Misana-ter Huurne et al., 2020).

The small body of literature that is available describes how entrepreneurs often take poor measures against cybercrime. For example, some entrepreneurs lack a cybersecurity policy, they tend to reuse the same password, and rarely have a separate Wi-Fi network for guests (Johns, 2021; Alert Online, 2019). Moreover, there is evidence that only a minority of the IT measures implemented by small businesses are designed and operated correctly, in addition to often being cheap and easy mitigations (Rohn et al., 2016; Osborn and Simpson, 2018). Thus, entrepreneurs show low levels of cyber resilience and are not prepared to prevent and recover from cyberattacks (Van der Kleij et al., 2019; Van der Kleij and Leukfeldt, 2019).

There are different views on the concept of cyber resilience in the literature (see for example Van der Kleij and Leukfeldt, 2019; Linkov and Kott, 2019), but our study emphasizes the social-psychological aspect. Herein, cyber resilience is defined as the combination of a sufficiently high degree of risk perception and self-protective behavior among citizens and entrepreneurs to prevent cybercrime victimization and/or to prevent or reduce its impact (Spithoven, 2020; Misana-ter Huurne et al., 2020). This perspective allows us to study the individual level and to identify specific behavioral components that can explain the high prevalence of ransomware victimization among entrepreneurs. It is important to gain more insight into cyber resilience from a psychological point of view, as it can offer the target group the prospect of modifying their lack of self-protective behavior. The aim of the current study is thus to explain why entrepreneurs should protect their businesses against ransomware in the future and to identify the factors influencing said motivation. To this end, we have applied an extended model of the Protection Motivation Theory (PMT; Rogers, 1975, 1983), derived from previous research. More knowledge on this matter can be used by government agencies, IT professionals and other parties involved in preventing cybercrime to help entrepreneurs become more cyber resilient.

In order to further scope out our recommendations, we also tested the model for two entrepreneur subgroups, namely those who do and do not outsource their IT security. The way in which entrepreneurs organize their IT security probably relates to their cyber resilience (e.g. Alwahdani, 2019; Osborn and Simpson, 2018). Therefore, differentiating between these subgroups leads to a better understanding of the factors that influence cybercrime victimization and protection among a heterogenous group of entrepreneurs.

2. Explaining cybercrime victimization using the PMT model

A lack of self-protective behavior might explain the high prevalence of ransomware victimization among entrepreneurs. With regard to cyber threats, security measures, such as firewalls, can be configured, and safe practices, for instance setting up suspicious activity alerts and recognizing suspicious requests, can be adopted. Previous research has sought to understand the differences in online security behaviors by means of the PMT. Originally developed by Rogers (1975) in the context of health behaviors, PMT offers a framework to explain the behavior of people protecting themselves from certain threats. Over the years, PMT and its constructs have been studied quite extensively in the context of online security behaviors, in which regard the theory seems to hold up well (e.g. Crossler and Bélanger, 2014; Tsai et al., 2016; De Kimpe et al., 2022; Jenkins et al., 2014; Van 't Hoff-de Goede et al., 2019; Safa et al., 2015; Hanus and Woo, 2016; Martens et al., 2019; Vance et al., 2012).

The theory asserts that precautionary behavior is motivated by an evaluation or appraisal of a certain threat (Rogers, 1975, 1983; Floyd et al., 2000). More specifically, threat appraisals include perceived vulnerability (i.e. estimates of the likelihood of being exposed to risk) and perceived severity (i.e. estimates of the severity of the possible effects of exposure). According to the theory, individuals need to believe that they are vulnerable to risks and they need to deem these risks as serious to comply with self-protective behaviors. In the context of online environments, it appears that threat appraisals tend to have a positive and direct effect on the conscientious online behavior of IT professionals (Safa et al., 2015). Mixed results are found when further distinguishing between perceived vulnerability and perceived severity. A higher estimated consequence of threats appeared to be associated with higher levels of security intentions, while no effect was found in the case of perceived vulnerability (Vance et al., 2012; Tsai et al., 2016). In another study based on a panel sample, both concepts were unrelated to the intention to install password management software (Menard et al., 2017). Conversely, De Kimpe et al. (2022) found a significant effect of both perceived severity and perceived vulnerability on the intention to adopt preventive measures. Therefore, because results are mixed, we chose to follow the PMT model and hypothesize the following:

H1. *Perceived severity is a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

H2. *Perceived vulnerability is a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

In addition to the threat appraisals performed by individuals, the effectiveness in coping with said threats can also be evaluated by means of the PMT (Rogers, 1975, 1983; Floyd et al., 2000). This so-called coping appraisal consists of three specific cognitive processes: self-efficacy, response efficacy and response costs. Coined by Bandura (1977), self-efficacy refers to the extent to which individuals consider themselves capable of actually adopting a certain form of behavior. Response efficacy is an assessment of the degree to which that behavior contributes to minimizing the risk, while response costs regard the perception of the cost (in terms of money, time and effort) of said behavior. Hence, according to the PMT, individuals must believe that they are capable of a recommended behavior; they need to perceive the behavior as useful and estimate that the benefits outweigh the costs. Note that response costs will not be included in the model of this study, because response costs overlap conceptually with self-efficacy and there is little need to measure both (Martens et al., 2019; De Kimpe et al., 2022; Sommestad et al., 2015).

Coping appraisals are also known to influence online self-protective behaviors. For instance, a higher degree of self-efficacy seems to be related to favorable security approaches, compliance with security policies and phishing threat avoidance behavior (Johnston and Warkentin, 2010; Herath and Rao, 2009; Arachchilage and Love, 2014; Crossler and Bélanger, 2014). Likewise, Tsai et al. (2016) have shown that the higher the response efficacy of an individual, the greater the intention to introduce online preventive measures. However, other studies imply that an increase in response efficacy and self-efficacy may be related to the decreased likelihood of entrepreneurs adopting measures; that is to say, some entrepreneurs believe that basic measures (e.g. backing up data) are sufficient to protect their companies (Ng et al., 2013; Osborn and Simpson, 2018). This means that entrepreneurs may overestimate their own abilities and the measures in use, and consider their businesses secure, while they are actually at risk of falling victim to cybercrime due to a lack of self-protective behaviors (e.g. Cheng et al., 2020; Riek et al., 2014). Indeed, in this sense, Tsai et al. (2016) found self-efficacy to be a negative predictor of security intentions. In another study, response efficacy also turned out to be negatively related to the intention to comply with security policies (Vance et al., 2012). In the specific case of entrepreneurs, Barlette et al. (2017) found both concepts to be unrelated to behavioral intention regarding information security. Again, because the results are inconsistent, we will adhere to the proposals of the PMT model (Rogers, 1975, 1983; Floyd et al., 2000):

H3. *Self-efficacy is a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

H4. *Response efficacy is a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

3. Extending the PMT model

While the traditional PMT model appears to be useful for explaining online self-protective behaviors, its factors are not entirely exhaustive and other variables play a role too. Therefore, for a more exhaustive understanding of cybercrime protection and the victimization of entrepreneurs, we have extended the PMT model with the addition of a number of variables (e.g. De Kimpe et al., 2022; Martens et al., 2019; Barlette et al., 2017).

To begin with, a lack of awareness of cybersecurity threats might be a key factor related to the motivation behind entrepreneurs' self-protective behaviors; that is, it appears that entrepreneurs often possess insufficient knowledge to protect their businesses and apply the necessary security measures, and they find it difficult to understand cyber threats and possible coping responses (Alahmari and Duncan, 2020; Huelsman et al., 2016; Ng et al., 2013; Osborn and Simpson, 2018; Osborn, 2014). Indeed, awareness of cybersecurity threats seems to be related indirectly to the intention to comply with self-protective behaviors. On the one hand, feeling more informed about cybercrime might result in individuals feeling more capable of applying measures and being more convinced they are effective, which, in turn, may increase self-protective behaviors (De Kimpe et al., 2022). On the other hand, studies have also found that greater perceived awareness about cybercrime may convince individuals that they are less vulnerable, resulting in the adoption of less measures (De Kimpe et al., 2022; Martens et al., 2019), although Martens et al. (2019) did not find such a link for malware specifically. Contrarily, said studies report a positive association with perceived severity: the greater the awareness, the more an individual perceives malware (Martens et al., 2019) and cybercrime in general (De Kimpe et al., 2022) as serious, even though the perceived likelihood of actually falling victim to an attack may be lower. Based on the aforementioned studies, we are proposing the following hypotheses:

H5. *Threat awareness is a positive predictor of entrepreneurs' perceived severity of ransomware.*

H6. *Threat awareness is a negative predictor of entrepreneurs' perceived vulnerability of ransomware.*

H7. *Threat awareness is a positive predictor of self-efficacy in entrepreneurs' self-protective behavior towards ransomware.*

H8. *Threat awareness is a positive predictor of response efficacy in entrepreneurs' self-protective behavior towards ransomware.*

Furthermore, while awareness about ransomware and cognitive appraisals found in the PMT model are likely to relate to self-protective behavior, the literature makes it clear that risk perception is not a mere cognitive assessment of the threat, i.e. experience or affect serve as cues to make judgement calls and operate in concordance with more rational decision-making (Slovic et al., 2004; Slovic and Peters, 2006). A different explanation for cybercrime victimization might thus be found in the experience of risk or, in other words, individuals' affective response. For example, using vignettes, Farshadkhah et al. (2021) showed that feelings of guilt may lower the intentions of employees to violate information security policies. Likewise, messages that appeal to the experience of fear, such as warnings about the consequences of reusing passwords, have been found to influence the intention of individuals to comply with cybersecurity norms (Johnston and Warkentin, 2010; Jenkins et al., 2014). Fear may also facilitate security behaviors against phishing (Bax et al., 2021; Jansen and Van Schaik, 2019). Thus, emotional responses can be triggered by social-environment stimuli, which in turn positively influence our online security behavior. It is, however, also possible that these stimuli lead to 'fear-control-processes', which means that people try to eliminate their feelings of fear, rather than the actual threat (e.g. Spithoven, 2017; Witte, 1992). Such processes are thought to be activated when the perceived threat is high, but perceived efficacy is low. This results in maladaptive responses, such as avoiding information and downplaying the risk, which might lower the intention of individuals to protect themselves. Thus, affective responses seem to be relevant factors worth considering, as also recommended by De Kimpe et al. (2022). Herein, our hypothesis is in line with the studies that have examined the relationship between affective responses and cybersecurity intentions (e.g. Farshadkhah et al., 2021; Jenkins et al., 2014; Bax et al., 2021).

H9. *Affective response is a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

A final perspective on the intention to engage in self-protective behavior considers the social environment of an individual. The concept of subjective norms stems from the Theory of Planned Behavior and refers to the perceived social encouragement or pressure to comply with or not to comply with certain behaviors (Ajzen, 1991). Subjective norms are formed by interpreting the beliefs of other groups or individuals. In the case of entrepreneurs, subjective norms may be invoked by managers, colleagues, other companies or individuals in their personal environment. It seems that the role of subjective norms is particularly valuable when studying entrepreneurs. Entrepreneurs may very well implement measures because they are advised to do so by their social ties (Barlette et al., 2017; Barlette and Jaouen, 2019). Martens et al. (2019) included subjective norms as a direct predictor of the intention to introduce cybersecurity measures and also found a significant positive effect. This is in line with other studies, as the perceived social norms on complying with information security policies in office settings predict the intention of employees to actually comply with those policies (Siponen et al., 2014; Ifinedo, 2014). Also, Lai et al. (2012) showed that the influence of individuals' social networks, i.e. family and friends, predicts their security intentions against identity theft.

H10. *Subjective norms are a positive predictor of entrepreneurs' intention to comply with self-protective behaviors against ransomware.*

In brief, research shows that cybercrime victimization might be the result of a combination of factors that go beyond the PMT model and that influence individuals' motivations to adopt self-protective behaviors. The less the self-protective behaviors of end users, the lower the cyber resilience, the more likely they will fall victim to cybercrime. Currently, little is known about the role of social-psychological factors in entrepreneurs' cyber resilience (e.g. Misana-ter Huurne et al. 2020; Barlette et al., 2017; Ng et al., 2013; Barlette and Jaouen, 2019; Osborn and Simpson, 2018). However, as shown in this literature overview, existing studies support the association between explanatory psychological factors and the motivation to adopt online security behaviors in a variety of populations and contexts. Therefore, we have tested an extended version of the protection motivation framework in a large sample of entrepreneurs, to examine if and how the intention to introduce self-protective behaviors towards ransomware can be explained.

4. Materials and methods

4.1. Data

Data were collected by distributing a questionnaire among a research agency panel consisting of 2000 Dutch entrepreneurs. Respondents received an accompanying email with information about the study and topic, as well as the link to the online questionnaire. During the period the questionnaire was open to respondents, an extra reminder was sent to entrepreneurs with staff in order to increase the representativeness of our sample. Completing the questionnaire took approximately fifteen minutes and no personal identifiable information was provided by respondents. Data were collected, stored and processed in accordance with the ethical regulations of the International Code on Market and Social Research (ICC, 2007), the Behavioral Code for Statistical and Analytical Research (MOA, 2022), the Golden Standard (MOA, 2020), and the General Data Protection Regulation (GDPR).

A total of 1020 entrepreneurs (response of 51%) completed the questionnaire. It appears that the demographics of our participants roughly match the broader population of entrepreneurs at SME level in the Netherlands, with the exception of educational level. There were slightly more male ($n = 570$; 55.8%) than female ($n = 441$; 43.2%) respondents. More than three quarters of the respondents were highly educated ($n = 770$; 75.5%; education level 'HBO' (i.e. Higher Vocational Education) or higher), which is more than the 50.4% average in Dutch SMEs (Statistic Netherlands, 2020). Of the participants, 80.4% ($n = 820$) were self-employed and the others had a business with staff, mostly with 1 to 10 employees. Most respondents were middle-aged ($n = 698$; 68.4%; 39 to 65 years), followed by 18 to 38 years ($n = 174$; 17.1%) and older than 65 years ($n = 148$; 14.5%). The majority of the respondents stated that they manage the IT security of their company internally, either themselves or with the help of an employee ($n = 679$; 66.6%), while about a third outsource their company's IT security ($n = 341$; 33.4%). Finally, respondents reported that they are operational in a variety of economic sectors, such as retail, food and the production industry. In total, a little under 20% ($n = 200$) stated that they had experienced an attempted ransomware attack at some point, while 1.5% ($n = 15$) of our sample had actually been victims of ransomware attacks in the past 12 months.

When zooming in on the subgroups, it was observed that in the case of entrepreneurs who manage their IT security internally, 89.1% ($n = 605$) are freelancers/self-employed, which is a little higher than the total sample, whereas 64.8% ($n = 221$) of them outsource. Also, those that outsource their IT security tend to be a little older than the total sample and the group who deals with IT security internally: 17% ($n = 58$) are over 65 and only 11.1% ($n = 38$) are in the 18–38 age group, as opposed to the 13.3% ($n = 90$) and 18.6% ($n = 126$) of entrepreneurs who are responsible for their own IT security. There are no other notable differences between the subgroups and the total sample in demographic terms.

4.2. Measures

An overview of the study's variables and measurements are listed in this section. These constructs and their items were derived from previous literature on social-psychological predictors of behavioral intention and the cyber resilience of entrepreneurs (e.g. De Kimpe et al., 2022; Martens et al., 2019; Misana-ter Huurne et al., 2020; Safa et al., 2015; Rogers, 1975, 1983). For the sake of this paper, the items have been translated into English by the authors of this study and a language editor. Pearson product-moment correlations between each item of a construct were calculated, which were all significant at the 0.001 level, and Cronbach's alpha (α) are listed to indicate internal consistency. Moreover, a principal component analysis with varimax rotation has been performed to identify the number of latent constructs and the underlying factor structure of the items of our variables, using Kaiser's criterion of eigenvalues greater than 1.

Dependent variable

The dependent variable in this study was the behavioral intention to take preventive measures against ransomware in the future. This was measured with three items, that correlate in the range of 0.75 to 0.84: "I feel I should do more to protect my business from ransomware attacks"; "I am planning to learn more about how I can prevent my business from falling victim to ransomware attacks"; "In the future I am going to take more measures to lower the threat of ransomware attacks on my business". This 5-point scale, ranging from "1=completely disagree" to "5=completely agree", proved to be reliable ($\alpha = 0.92$). Factor loading ranged from 0.91 to 0.94 with an Eigenvalue of 2.57 that explained 85.7% of the variance. Behavioral intention was chosen over self-protective behavior as the dependent variable because the study was unable to measure actual behavior due to practical constraints.

Independent variables

The following constructs were measured as independent variables. Items were measured on a 5-point Likert scale, generally ranging from "1 = strongly disagree" to "5 = strongly agree" (exceptions are listed where needed).

Perceived vulnerability. Perceived vulnerability was measured using one item: "How likely is it your business would fall victim to a ransomware attack in the next 12 months?" ("1 = highly unlikely" to "5 = highly likely").

Perceived severity. Perceived severity was measured using two items on the effect of victimization ("If my business were to fall victim to a ransomware attack, it would cause considerable harm to my business (in terms of money, time or privacy)"; "If my business were to fall victim to a ransomware attack, it would have a considerable emotional impact on me"). The items, which were highly correlated ($r = 0.56$), also proved reliable ($\alpha = 0.72$). Both items had factor loadings of 0.88 with an Eigenvalue of 1.56 that explained 78% of the variance.

Self-efficacy. Self-efficacy was measured based on four statements': "'I am capable of estimating the risks for my business if it falls victim to a ransomware attack"; "I am capable of protecting my business against a ransomware attack"; "I am capable of recognizing a ransomware attack"; "I am capable of doing what needs to be done when my business falls or appears to fall victim to a ransomware attack". In this case, response categories ranged from "1=not at all" to "5=completely". Items showed a Pearson's correlation of 0.61 up to 0.73 and the scale proved reliable at $\alpha = 0.88$. The factor analysis showed that the items can explain 73.8% of the variance with factor loadings ranging from 0.84 to 0.90 and an Eigenvalue of 2.95.

Response efficacy, measured using three items: "Being aware and taking measures helps to protect your business from ransomware attacks", "With the measures my business has taken, my business is less likely to fall victim to a ransomware attack" and "With the measures my business has taken, it would be less impacted were it to fall victim to a ransomware attack". The item-total correlation ranged from 0.41 to 0.70, with a Cronbach's alpha of 0.79. The factor loadings ranged from 0.75 to 0.90, and explained 70% of the variance with an Eigenvalue of 2.10.

Threat awareness. Threat awareness was measured using three statements ("I know how my business could fall victim to ransomware attacks"; "I know how hackers can install ransomware on my business devices"; "I know what can happen if ransomware is installed on my business devices"). These items were highly correlated (ranging from 0.74 to 0.79) and showed good internal consistency ($\alpha = 0.81$). The factor loadings ranged from 0.912 to 0.932. The Eigenvalue of 2.540 was able to explain 84.7% of the variance.

Affective response. Affective response was measured by two statements, ranging from "1=not at all" to "5 = a lot" ("How concerned are you about your business falling victim to a ransomware attack?"; "How concerned are you about your business being harmed as a result of a ransomware attack?"). With a strong correlation of 0.80, the items showed a Cronbach's alpha of 0.70, with factor loadings of 0.95. An Eigenvalue of 1.80 was reported, and an explained variance of 90.1%.

Subjective norms. Subjective norms were measured with two items ($r = 0.54$; $\alpha = 0.70$): "Companies in our sector find it important that my business protect itself against cybercrime" and "I tend to protect my company against cybercrime because it is expected of me". The factor loadings of these items are 0.88. An Eigenvalue of 1.54 explained 77% of the variance.

4.3. Analysis

Mean scores and assumed coherence (correlations) between concepts from the model were calculated and analyzed in SPSS. The conceptual model was tested by means of Structural Equation Modeling (SEM) using AMOS software, providing insight into which factors influence the intention of entrepreneurs to show self-protective behaviors in the future. Structural Equation Modeling is an integration of various statistical techniques, such as regression analysis, factor analysis and scale constructions. This allows interrelationships between concepts to be calculated in a detailed manner that explicitly consider interdependence and the interrelationship of multiple variables (Hox and Bechger, 1998; Bollen and Pearl, 2013).

The suitability of the model was tested on the basis of so-called fit indices. The Chi-square ($\chi 2$) measured the discrepancy between the estimated model-implied covariance matrix of the population and sample covariance matrix. The Comparative Fit Index (CFI) was used to evaluate the model fit. It relies on the average correlations of variables in the model. Values range from 0 to 1, in which values of 0.90 or higher are recommended (Bentler, 1990). The Root Mean Square Error of Approximation (RMSEA) also includes the sample size. Values below .05 imply a good fit, values between 0.05 and 0.08 are considered an adequate fit and values between 0.08 and 0.10 a mediocre fit (Browne and Cudeck, 1993).

As already stated, for a more in-depth understanding of the cyber resilience of entrepreneurs, we ran the model for two subgroups too: those who outsource their IT security (i.e. "external IT security") and those who do not (i.e. "internal IT security"). Other comparisons between subgroups, such as entrepreneurs with employees as opposed to freelancers, had too few respondents for the SEM analysis to be performed.

Table 1
Overview of variable scores.

Variables	Mean score (scale: 1 to 5)	Standard deviation (SD)
Perceived severity	3.81	0.91
Perceived vulnerability	2.15	0.83
Self-efficacy	3.19	0.84
Response efficacy	3.68	0.75
Threat awareness	3.34	1.06
Affective response	2.44	0.96
Subjective norms	3.37	0.93
Behavioral intention	3.05	0.87

5. Results

5.1. Overall descriptives

Table 1 shows the mean scores and standard deviations of the measured variables regarding ransomware attacks for all respondents ($n = 1020$).

For the respondents, the likelihood of them falling victim to an attack is relatively low ($M = 2.15$). Possible damage to their businesses and the emotional impact of a ransomware attack are estimated to be higher ($M = 3.81$). As for coping appraisals, the mean score on response efficacy (3.68) is higher than the mean score on self-efficacy ($M = 3.19$). The average score on awareness about the risks of ransomware is 3.34, while participants scored an average of 2.44 when asked about their concerns regarding the risk of falling victim to a ransomware attack. A mean score of 3.37 was calculated in the case of subjective norms. Lastly, entrepreneurs are neutral about introducing measures to protect their businesses against ransomware attacks in the future ($M = 3.05$).

As for wanting more information on ransomware, 41% ($n = 422$) of respondents stated they were interested, especially on how they can protect their businesses. Entrepreneurs also listed the barriers they come across when introducing measures to prevent cybercrime: 38.9% ($n = 397$) find taking measures to be too complicated, 37.2% ($n = 379$) are convinced taking additional measures would not protect their businesses and 33.7% ($n = 344$) reported that taking measures is time-consuming. Despite these obstacles, the respondents scored an average of 4.29 (SD = 0.55) on a 5-point scale on current self-reported, self-protective behavior regarding ransomware.

An overview of the correlations between all the measured variables is presented in Table 2. The strongest correlations were found between response efficacy and self-efficacy ($r = 0.64$) and between affective response and perceived vulnerability ($r = 0.52$). Subjective norms were the only variables not significantly related to behavioral intention, the dependent variable of our study. In all other cases, self-efficacy, response efficacy and threat awareness showed a negative association with behavioral intention, while perceived severity, perceived vulnerability and affective response were positively correlated (Fig. 1).

5.2. Model test

The results from the model test for the total sample are presented in Fig. 2. The model, based on an exploratory set of variables and measurements, showed a fit around the mediocre range ($n = 1020$; RSMEA $= 0.088$; CFI $= 0.89$; $\chi^2(158)=1413.87$, $p < .001$). An overview of the implications of these findings for this paper's hypotheses is shown in Table 3.

It appeared that the intention to engage in self-protective behavior is influenced significantly by all five direct predictors. Affective response ($\beta = 0.291$, $p < .001$) and self-efficacy ($\beta = -0.273$, $p < .001$) were the strongest direct predictors. While affective re-

Table 2
Correlation between model variables.

	1	2	3	4	5	6	7
(1) Perceived severity	–						
(2) Perceived vulnerability	0.23***	–					
(3) Self-efficacy	−0.20***	−0.28***	–				
(4) Response efficacy	−0.14***	−0.27***	0.64***	–			
(5) Threat awareness	−0.06	−0.12***	−0.14***	0.49***	–		
(6) Affective response	0.41***	.52***	−0.21***	−0.16***	0.01	–	
(7) Subjective norms	0.05	−0.02	0.31***	0.41***	0.31***	0.09**	–
(8) Behavioral intention	0.31***	.34***	−0.37***	−0.29***	−0.22***	0.41***	0.03

$^{*}p$ <.05. $^{**}p$ <.01. $^{***}p$<.001.

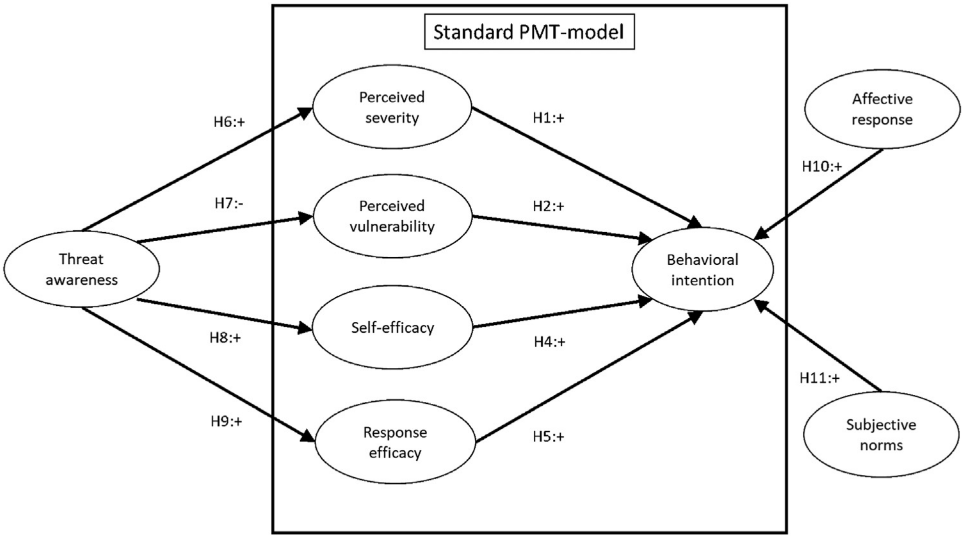

Fig. 1. Schematic overview of the extended PMT model and expected links.

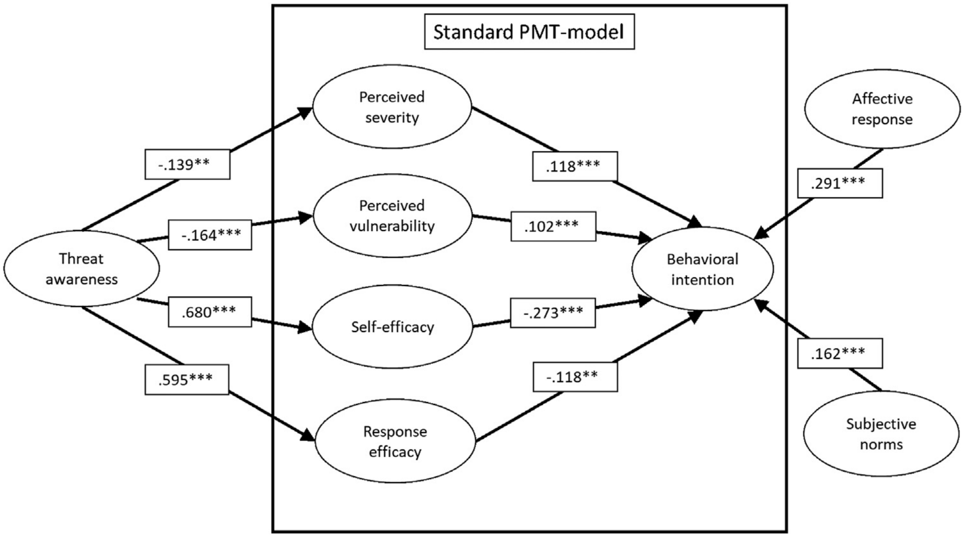

Fig. 2. Schematic overview of model test based on total sample.
$^{*}p$ < .05. $^{**}p$ < .01. $^{***}p$ < .001.

sponse positively affects the intention of entrepreneurs to take preventive measures against ransomware, self-efficacy negatively affected said intention. This means that entrepreneurs are more likely to take additional measures when they are more concerned about their own risks (affective response) and when they consider themselves less capable of performing self-protective behavior (self-efficacy). We expected to find the first relationship, but the latter contradicted our hypotheses. Moreover, response efficacy also showed a significant negative relationship with behavioral intention, while we expected a positive relationship (β = −0.118, p <.01). In other words, a stronger belief in the efficacy of measures reducing ransomware threats makes entrepreneurs less inclined to take measures.

The threat appraisals from the original PMT model were significant positive predictors of the intention to protect a business against ransomware attacks (perceived severity: β=0.118, p<.001; perceived vulnerability: β=0.102, p<.001). Thus, the more entrepreneurs believe they risk becoming ransomware attack victims

Table 3
Overview of hypotheses and model test results based on total sample (n = 1020).

From	To	Hypotheses	β	H confirmed
Perceived severity	Behavioral intention	H1: +	.118***	Yes
Perceived vulnerability	Behavioral intention	H2: +	.102***	Yes
Self-efficacy	Behavioral intention	H3: +	−0.273***	No
Response efficacy	Behavioral intention	H4: +	−0.118**	No
Threat awareness	Perceived severity	H5: +	−0.139**	No
Threat awareness	Perceived vulnerability	H6: -	−0.164***	Yes
Threat awareness	Self-efficacy	H7: +	.680***	Yes
Threat awareness	Response efficacy	H8: +	.595***	Yes
Affective response	Behavioral intention	H9: +	.291***	Yes
Subjective norms	Behavioral intention	H10: +	.162***	Yes

* $p < .05$. ** $p < .01$. *** $p < .001$.

Table 4
Overview of hypotheses and results in model test of "external IT security" subgroup (n = 341).

From	To	Hypotheses	β	H confirmed
Perceived severity	Behavioral intention	H1: +	0.121*	Yes
Perceived vulnerability	Behavioral intention	H2: +	0.055 (ns)	No
Self-efficacy	Behavioral intention	H3: +	−0.270***	No
Response efficacy	Behavioral intention	H4: +	−0.183**	No
Threat awareness	Perceived severity	H5: +	−0.170*	No
Threat awareness	Perceived vulnerability	H6: -	−0.170**	Yes
Threat awareness	Self-efficacy	H7: +	0.706***	Yes
Threat awareness	Response efficacy	H8: +	0.549***	Yes
Affective response	Behavioral intention	H9: +	0.293***	Yes
Subjective norms	Behavioral intention	H10: +	.061 (ns)	No

* $p < .05$. ** $p < .01$. *** $p < .001$.

Table 5
Overview of hypotheses and results in model test of "internal IT security" subgroup (n = 679).

From	To	Hypotheses	β	H confirmed
Perceived severity	Behavioral intention	H1: +	0.100**	Yes
Perceived vulnerability	Behavioral intention	H2: +	0.128**	Yes
Self-efficacy	Behavioral intention	H3: +	−0.289***	No
Response efficacy	Behavioral intention	H4: +	−0.048	No
Threat awareness	Perceived severity	H5: +	−0.128*	No
Threat awareness	Perceived vulnerability	H6: -	−0.164***	Yes
Threat awareness	Self-efficacy	H7: +	0.670***	Yes
Threat awareness	Response efficacy	H8: +	0.623***	Yes
Affective response	Behavioral intention	H9: +	0.301***	Yes
Subjective norms	Behavioral intention	H10: +	0.181***	Yes

$^{*}p < .05$. $^{**}p < .01$. $^{***}p < .001$.

and the more they believe that victimization can have severe consequences, the more inclined they are to implement additional measures. Both findings were in line with our hypotheses. Lastly, as expected, social environment influence related significantly and positively to behavioral intention (β = 0.162, p <.001): the more entrepreneurs are convinced that other people feel they should protect their businesses and the more likely they are to conform to this subjective standard, the greater the intention to take measures.

Other factors were indirectly associated with behavioral intention. On the one hand, the coping appraisals – self-efficacy and response efficacy - were both strongly and positively influenced by awareness about the risks of ransomware, thereby confirming the associated hypotheses (β=0.680, p<.001 and β=0.595, p<.001 respectively). Thus, the more entrepreneurs believe they know about the risks of ransomware, the more they consider themselves capable of protecting their companies against ransomware attacks and the more they are convinced such behavior is effective in mitigating the risk. On the other hand, threat awareness showed a significant negative relation with perceived severity and perceived vulnerability of ransomware victimization (β = −0.139, p < .01 and β = −0.164, p < .00, respectively): the higher the degree of awareness about the risks of ransomware, the less entrepreneurs perceive ransomware as a threat to their companies in terms of vulnerability and severity. This was partly in line with our expectations.

5.3. Model test for subgroups

The results of the model test for the two entrepreneur subgroups are described in Table 4, Fig. 3, Table 5 and Fig. 4. In the case of entrepreneurs who outsource their companies' IT security (n = 341), the model showed a fit around the mediocre range (RSMEA = 0.090; CFI = 0.884; $\chi^2(158)$ = 596.86, p <.001). The same goes for entrepreneurs who handle IT security internally (n = 679; RSMEA = 0.089; CFI = 0.892; $\chi^2(158)$ = 1001.82, p <.001).

Overall, the relationships between the independent and dependent variables in the case of the subgroups were comparable to those of all the respondents together, although differences were found. Regarding the internal IT security group, response efficacy was not significantly associated with behavioral intention, in contrast to the total sample and the entrepreneurs who outsource. In the case of the entrepreneurs who hire an external company, two key differences were observed compared to the other groups: both

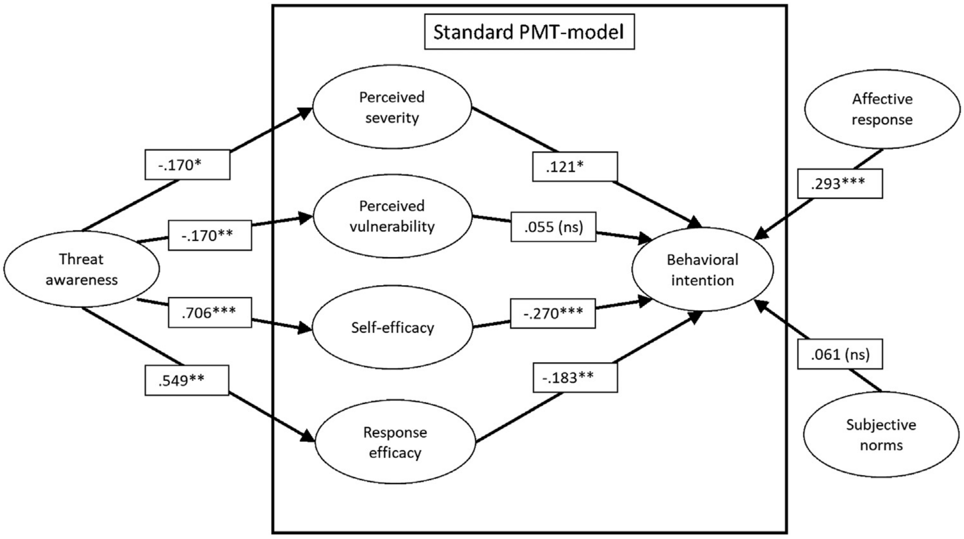

Fig. 3. Schematic overview of model test of “external IT security” subgroup.
$^{*}p < .05$. $^{**}p < .01$. $^{***}p < .001$.

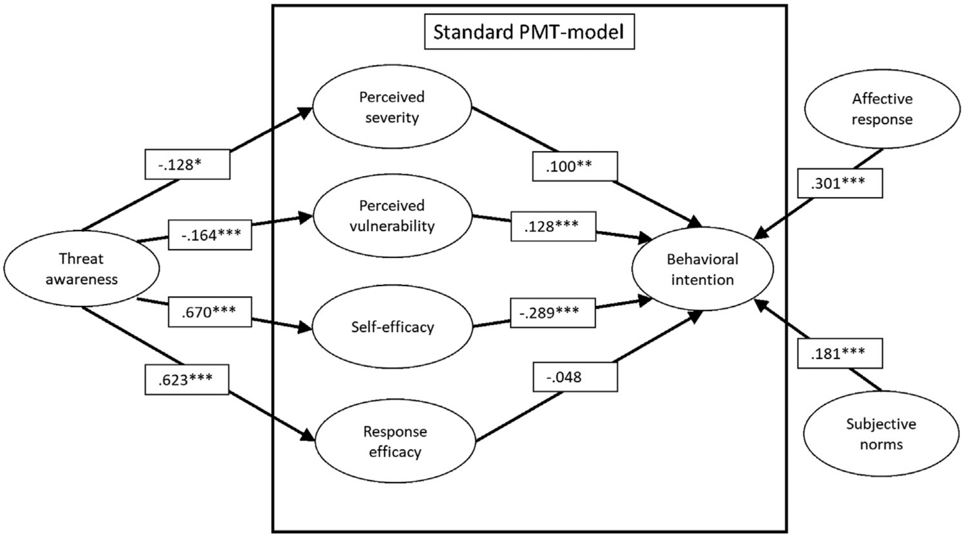

Fig. 4. Schematic overview of model test of “internal IT security” subgroup.
$^{*}p < .05$. $^{**}p < .01$. $^{***}p < .001$.

perceived vulnerability and subjective norms showed no significant association with behavioral intention.

6. Discussion

The aim of this paper was to identify the underlying social-psychological factors that explain entrepreneurs' motivations for taking preventive measures against ransomware attacks. To achieve said aim, a questionnaire was distributed among a sample from a panel bureau and was completed by 1020 Dutch freelancers and owners of small- and medium-sized enterprises (SMEs) with up to 250 employees. We used an extended version of the PMT model, in which subjective norms and affective response were added as the direct predictors of behavioral intention and threat awareness as an indirect predictor. Our dataset provided insight into a population that is rather vulnerable to cybercrime, but difficult to access for research purposes.

Descriptives show that entrepreneurs generally perceive little risk of their businesses falling victim to ransomware attacks, which does not align with the notion that entrepreneurs are targeted rather often (e.g. Leukfeldt, 2018; Notté et al., 2019; Veenstra et al., 2015). In particular, scores on perceived vulnerability are notably low (e.g. Wilson et al., 2022). Similarly, high scores on current self-protective behavior imply that entrepreneurs are (erroneously) convinced that their businesses are protected. This may indicate the presence of optimistic bias: people generally perceive their own online risk to be lower than those of other comparable individuals, which may demotivate individuals from adopting self-protecting behaviors (Rhee et al., 2005, 2012). People generally appear to be unable to accept their own vulnerability towards virtually all risks they face in contemporary life (Spithoven, 2017). Thus, the presence and role of optimistic bias in the online security behaviors of entrepreneurs is an avenue worth pursuing in future research efforts.

Thanks to our SEM analysis, we determined that the intention to take more self-protective measures in the future is higher when entrepreneurs are concerned about risks (affective response) and when they believe that people in their environment expect them to take self-protective measures (subjective norms). This was in line with our expectations (e.g. Johnston and Warkentin, 2010; Jenkins et al., 2014; Siponen et al., 2014; Ifinedo, 2014; Barlette et al., 2017). The role of affective response indicates that being concerned about cybercrime might actually motivate entrepreneurs to protect their businesses. This was the strongest direct predictor of behavioral intention for the total sample as well as the subgroups, thus explaining the motivation of entrepreneurs regardless of whether they are outsourcing IT or not. Moreover, it seems that entrepreneurs' interactions with their social environment influence their decision-making in terms of cybersecurity, which implies that entrepreneurs can be extrinsically motivated to perform such behaviors.

Contrary to our hypotheses, entrepreneurs seem less likely to protect their companies in the future if they believe that they are able to do so already (self-efficacy) and if they are convinced that taking measures actually helps to minimize the risk (response efficacy). These findings might be explained by the notion that entrepreneurs who score high on coping appraisals overestimate their abilities and the measures they have already taken and thus see no need in taking additional measures, which is reflected in the high scores on current, self-reported, self-protective behavior in our sample. This is in line with the "overconfidence hypotheses" (Cheng et al., 2020; Riek et al., 2014): those with higher efficacy beliefs regarding the use of IT devices can be more susceptible to cybercrime victimization because they tend to be online more frequently and are less likely to avoid (risky) online services. Thus, as soon as entrepreneurs think they can protect their companies against ransomware attacks, their risk perception drops. We recommend that future research studies investigate entrepreneurs' overconfidence in cybersecurity behaviors further.

Regarding the threat appraisals, our analysis revealed that both perceived severity and perceived vulnerability were positively related to behavioral intention: entrepreneurs who deem it likely they will fall victim to ransomware attacks and who find the consequences of victimization severe, plan on protecting their businesses better against ransomware attacks in the future. This is in line with our hypothesis (e.g. Safa et al., 2015; Vance et al., 2012; Tsai et al., 2016; De Kimpe et al., 2022).

Let us now turn to the indirect predictor of behavioral intention, namely threat awareness. Firstly, more awareness about ransomware seems to negatively influence both threat appraisals. This is partly in line with our hypothesis. While we expected higher scores on threat awareness to be associated with a decrease in perceived vulnerability (e.g. Martens et al., 2019; De Kimpe et al., 2022), we did not expect a negative relationship with perceived severity. The latter might be explained with the notion of overconfidence (Cheng et al., 2020; Riek et al., 2014), which also explains the decreased sense of vulnerability: more information about the risks of ransomware leads to overestimating the ability to avoid the consequences of what it can lead to. This means that feeling informed about ransomware may not only make entrepreneurs think they are immune to an attack, but also lead them to see less of a threat in terms of the emotional or financial impact of an attack, which in turn lowers their intention to comply with self-protective behaviors. It may also be that our measurements of threat awareness and the coping appraisals overlap conceptually, thereby explaining the strong association between them.

Secondly, besides the influence of awareness on the threat appraisals, our findings confirmed the expectation that more awareness regarding ransomware is associated with stronger beliefs about entrepreneurs' capabilities to protect their own companies (self-efficacy) and about the effectiveness of their measures against ransomware (response efficacy). Indeed, the effect of threat awareness on self-efficacy and response efficacy revealed the strongest relationships in our analysis overall. However, whether that is a good thing or not is debatable, given that a higher degree of self-efficacy and response efficacy is associated with a decline in the intention to engage in self-protective behaviors.

When zooming in on the entrepreneur subgroups, we found that hiring an external company for IT security is associated with a decreased effect size of subjective norms and perceived vulnerability on behavioral intention, to the point of insignificance. In other words, entrepreneurs who outsource IT security think they are less vulnerable to cybercrime and are less influenced by their social environment than those who do not outsource their IT security. This might be explained by the notion that entrepreneurs trust in the expertise of the external company and consider their businesses to be safe and in good hands (e.g. Van den Berg and Keymolen, 2017; Alwahdani, 2019; Osborn and Simpson, 2018). However, this might be a vulnerability: outsourcing security does not necessarily mean that a company is well-protected. For instance, the level of protection also depends on specific arrangements with the IT security company and the degree of compliance with security policies by employees, regardless of the specific measures adopted by the external experts (e.g. Safa et al., 2015; Alwahdani, 2019).

6.1. Practical and theoretical implications

Our extended PMT model seems to predict, in part, the cyber resilience of entrepreneurs. We identified a number of social-psychological factors that might contribute to the relatively high numbers of cybercrime victimization among the target group. The specific findings of this study therefore provide a number of starting points for actions that information security professionals, policy makers or other parties involved in cybercrime prevention can adopt to increase the cyber resilience of entrepreneurs against cybercrime. These implications essentially hold true for the prevention of ransomware attacks, but it can be argued that they also apply to cybercrime in general, particularly to other forms of malware. Generalizing our results in relation to cybercrimes other than ransomware would, however, require additional research.

A first point is that caution should be exercised when informing entrepreneurs about the risks of ransomware (see also Bada et al., 2019). Results indicate that more knowledge about the risks may lead to underestimating the likelihood and impact of ransomware attacks, and simultaneously to overestimating the effectiveness of adopted measures and one's own ability to protect the company. In both cases, this lowers the chances of entrepreneurs complying with self-protective behaviors. It may be more useful informing entrepreneurs on how to cope with ransomware and to stress why this is relevant for their company; or showing entrepreneurs how they can take targeted action and which measures they can introduce to prevent ransomware attacks and victimization. It is important that these measures be user-friendly in terms of time and complexity, as entrepreneurs often seem to think cybersecurity measures are too complicated, take too much time or are too expensive. In this sense, it is essential that evidence-based communication strategies about cybersecurity be considered, for instance by paying attention to the reliability of the message and discouraging neutralization techniques that lead to non-compliance (see also Nurse et al., 2011; Barlow et al., 2013).

By the same token, an issue that arises from our findings is that entrepreneurs have a low risk perception, particularly a low estimated likelihood of becoming victims themselves. Findings imply that a high degree of perceived severity and perceived vulnerability might motivate entrepreneurs to take more measures. Interventions should therefore focus on increasing personal risk perception and reduce the target audience's optimistic bias. The message that any entrepreneur and their business can fall victim to ransomware attacks, and that these can often lead to financial and emotional damage, might trigger self-protective behaviors.

In addition, subjective norms and affective responses need to be addressed as direct influencers of self-protective behavior. If entrepreneurs are convinced that companies in their professional environment exhibit safe behavior, and their close network expects them to do so as well, they may be more inclined to display self-protective behavior (e.g. Siponen et al., 2014; Ifinedo, 2014). This may be a relevant strategy especially in the case of entrepreneurs who outsource. The same is true for fear-appeal-based communication used to elicit emotional responses from individuals, for instance by addressing the likelihood of victimization, given that perceived vulnerability and affective response are strongly correlated (Johnston and Warkentin, 2010; Jenkins et al., 2014). Eliciting an affective response from entrepreneurs is especially important, as this was the strongest direct predictor of the intention to take measures against ransomware in the future.

Finally, we found evidence that outsourcing IT security is associated with a lower motivation to comply with self-protective behaviors, because entrepreneurs see cybercrime as less of a threat for their companies and are less likely to be encouraged by their social environment. It is thus important that security companies maintain an honest and open relationship with entrepreneurial clients, in which it is stressed that entrepreneurs still have a responsibility to protect their own company and have to behave accordingly in order to prevent victimization (e.g. Alwahdani, 2019).

6.2. Limitations and future research

Our study was based on a unique and large dataset of a research group that is usually hard to reach. With our results, we are contributing to the limited knowledge on the goal-oriented motivations and behaviors of entrepreneurs regarding cybersecurity. Nevertheless, the findings of this study should be considered in the light of some (methodological) limitations. A first point is that we considered self-reported behavioral intention as the most important direct predictor of actual behavior, in line with such theoretical models as PMT. In the field of cyber resilience, the relationship between behavioral intentions and actual behavior has received little attention. However, empirical evidence supporting this relationship has been found in other research domains and populations (see also Sheeran, 2002; Webb and Sheeran, 2006). Future research could investigate further the extent to which explanatory factors can predict actual self-protective behaviors regarding cybercrime by means of (experimental) effect measurements. Secondly, although the sample was large ($n = 1020$), a self-selection was possible for certain groups of entrepreneurs given the response rate of 51% and the fact that respondents had agreed to be on a panel. This is reflected in the fact that our respondents had a higher education level than the broader population of entrepreneurs in the Netherlands. Currently, not much is known about the cyber resilience of specific groups of entrepreneurs and the role of certain characteristics. We encourage future research to consider different sectors, demographics and internal business processes such as organizational culture to explain self-protective behavior. Finally, the construct of threat awareness needs further examination. In our study, it may have reflected the same underlying construct as the two coping appraisals, considering the strong influence of threat awareness on self-efficacy and response efficacy. It is important to examine other forms of awareness and to apply different measurements of this construct, for instance by testing actual knowledge.

7. Conclusion

In this study, we sought to explain the intention of entrepreneurs to take preventive measures against ransomware attacks in the future. Currently, ransomware is a major threat in the cybersecurity ecosystem, especially in the case of small- and medium-sized enterprises. At the same time, entrepreneurs are known to generally lack self-protective behavior online. This makes entrepreneurs a valuable target group for research purposes. With our extended PMT model, we found that the motivation to protect one's business against ransomware may be explained by a complex interplay of various social-psychological factors. In order to prevent victimization, it is important that information security professionals use the findings of this study to increase the cyber resilience of entrepreneurs. Evidence-based behavioral intervention is pivotal to protecting vulnerable groups of individuals against the ever-growing threat of cybercrime.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Remco Spithoven reports financial support was provided by SIA, part of The Dutch Research Council.

CRediT authorship contribution statement

Luuk Bekkers: Validation, Writing – original draft, Writing – review & editing, Visualization. **Susanne van 't Hoff-de Goede:** Methodology, Writing – review & editing, Conceptualization. **Ellen Misana-ter Huurne:** Methodology, Formal analysis, Writing – review & editing, Data curation. **Ynze van Houten:** Writing – review & editing. **Remco Spithoven:** Conceptualization, Supervision, Funding acquisition, Writing – review & editing. **Eric Rutger Leukfeldt:** Conceptualization, Supervision, Funding acquisition, Writing – review & editing.

Data availability

Data will be made available on request.

Acknowledgements

This study was supported by the Taskforce for Applied Research SIA of the Dutch Research Council [Grant number RAAK.PUB06.032].

References

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process 50 (2), 179–211. doi:10.1016/0749-5978(91)90020-T.

Alahmari, A., Duncan, B., 2020. Cybersecurity risk management in small and medium-sized enterprises: a systematic review of recent evidence. In: International Conference on Cyber Situational Awareness, Data Analytics and Assessment. IEEE, pp. 1–5. doi:10.1109/CyberSA49311.2020.9139638.

Alwahdani, A, 2019. The impact of trust and reciprocity on knowledge exchange: a case study in IT outsourcing. J. Inform. Syst. Eng. Manage. 4 (1), em0084. doi:10.29333/jisem/5738.

Alert Online. (2019). Nationaal Cybersecurity Bewustzijnsonderzoek 2019. https://www.alertonline.nl/media/Alert-Online-Cybersecuritybewustzijnsonderzoek-2019-2.pdf.

Arachchilage, N.A.G., & Love, S. (2014). Security awareness of computer users: a phishing threat avoidance perspective. *Comput. Hum. Behav.*, 38, 304–312. doi:10.1016/j.chb.2014.05.046.

Bada, M., Sasse, A.M., Nurse, J.R., 2019. Cyber Security Awareness campaigns: Why do They Fail to Change Behaviour?. arXiv preprint arXiv:1901.02672doi:10.48550/arXiv.1901.02672.

Bandura, A., 1977. Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. 84 (2), 191–215. doi:10.1037/0033-295X.84.2.191.

Barlette, Y., Gundolf, K., Jaouen, A., 2017. CEOs' information security behavior in SMEs: does ownership matter? Syst. Inform. Manage. 22 (3), 7–45. doi:10.3917/sim.173.0007.

Barlette, Y., Jaouen, A., 2019. Information security in SMEs: determinants of CEOs' protective and supportive behaviors. Syst. Inform. Manage. 24 (3), 7–40. doi:10.3917/sim.193.0007.

Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A.R., 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. Comput. Secur. 39, 145–159. doi:10.1016/j.cose.2013.05.006.

Bax, S., McGill, T., Hobbs, V., 2021. Maladaptive behaviour in response to email phishing threats: the roles of rewards and response costs. Comput. Secur. 106, 102278. doi:10.1016/j.cose.2021.102278.

Bentler, P.M., 1990. Comparative fit indexes in structural models. Psychol. Bull. 107 (2), 238–246. doi:10.1037/0033-2909.107.2.238.

Bollen, K.A., Pearl, J., 2013. Eight myths about causality and structural equation modeling. In: Morgan, S.L. (Ed.), Handbook of Causal Analysis For Social Research. Springer, pp. 301–328.

Browne, M.W., Cudeck, R., 1993. Alternative ways of assessing model fit. In: Bollen, K.A., Long, J.S. (Eds.), Testing Structural Equation Models. Sage, pp. 136–162.

Cheng, C., Chan, L., Chau, C.L., 2020. Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Comput. Hum. Behav. 108, 106311. doi:10.1016/j.chb.2020.106311.

Crossler, R., Bélanger, F., 2014. An extended perspective on individual security behaviors: protection motivation theory and a unified security practices (USP) instrument. ACM SIGMIS Database 45 (4), 51–71. doi:10.1145/2691517.2691521.

De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K., 2022. What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behav. Inf. Technol. 41 (8), 1796–1808. doi:10.1080/0144929X.2021.1905066.

Farshadkhah, S., Van Slyke, C., Fuller, B., 2021. Onlooker effect and affective responses in information security violation mitigation. Comput. Secur. 100, 102082. doi:10.1016/j.cose.2020.102082.

Floyd, D.L., Prentice-Dunn, S., Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. J. Appl. Soc. Psychol. 30 (2), 407–429. doi:10.1111/j.1559-1816.2000.tb02323.x.

Hanus, B., Wu, Y.A., 2016. Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Inform. Syst. Manage. 33 (1), 2–16. doi:10.1080/10580530.2015.1117842.

Herath, T., Rao, H., 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. Eur. J. Inform. Syst. 18 (2), 106–125. doi:10.1057/ejis.2009.6.

Hox, J.J., Bechger, T.M., 1998. An introduction to structural equation modelling. Fam. Sci. Rev. 11, 354–373.

Huelsman, T., Powers, E., Peasly, S., Robinson, R. (2016). Cyber risk in advanced manufacturing. Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/manufacturing/us-manu-cyber-risk-in-advanced-manufacturing.pdf.

Ifinedo, P., 2014. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. Inform. Manage. 51 (1), 69–79. doi:10.1016/j.im.2013.10.001.

International Chamber of Commerce (ICC). (2022). ICC/Esomar international code on market and social research. https://iccwbo.org/content/uploads/sites/3/2008/01/ESOMAR-INTERNATIONAL-CODE-ON-MARKET-AND-SOCIAL-RESEARCH.pdf.

Jansen, J., van Schaik, P., 2019. The design and evaluation of a theory-based intervention to promote security behaviour against phishing. International Journal of Human-Computer Studies 123, 40–55. doi:10.1016/j.ijhcs.2018.10.004.

Jenkins, J.L., Grimes, M., Proudfoot, J.G., Lowry, P.B., 2014. Improving password cybersecurity through inexpensive and minimally invasive means: detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. Inform. Technol. Dev. 20 (2), 196–213. doi:10.1080/02681102.2013.814040.

Johns, E., 2021. *Cyber Security Breaches Survey*. Department for Digital. Culture, Media & Sport https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021.

Johnston, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 548–566. doi:10.2307/25750691.

Lai, F., Li, D., Hsieh, C.T., 2012. Fighting identity theft: the coping perspective. Decis. Support Syst. 52 (2), 353–363. doi:10.1016/j.dss.2011.09.002.

Leukfeldt, R. (2018). *De 'human' factor in cybersecurity: intreerede.* De Haagse Hogeschool. https://www.narcis.nl/publication/RecordID/oai:hbokennisbank.nl:sharekit_hh%3Aoai%3Asurfsharekit.nl%3Aee64660b-45f1-4018-af0b-ca36bc93c518.

Linkov, I., Kott, A., 2019. Fundamental Concepts of Cyber Resilience: introduction and Overview. In: Kott, A., Linkov, I. (Eds.), Cyber Resilience of Systems and Networks. Risk, Systems and Decisions. Springer, pp. 1–25. doi:10.1007/978-3-319-77492-3_1.

Marktonderzoek Associatie (MOA). (2020). Gebruikersinstructie Gouden Standaard. https://www.moa.nl/images/MOAweb/bestanden/Gebruikersinstructie_GS2020_dec2020.pdf.

Marktonderzoek Associatie (MOA). (2022). Gedragscode voor statistisch onderzoek 2022. https://sharedpictures.moaweb.nl/images/Gedragscode-2022.pdf.

Martens, M., De Wolf, R., De Marez, L., 2019. Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Comput. Hum. Behav. 92, 139–150. doi:10.1016/j.chb.2018.11.002.

Menard, P., Bott, G.J., Crossler, R.E., 2017. User motivations in protecting information security: protection motivation theory versus self-determination theory. J. Manage. Inform. Syst. 34 (4), 1203–1230. doi:10.1080/07421222.2017.1394083.

Misana-ter Huurne, E., Van Houten, Y., Spithoven, R., Notté, R., & Leukfeldt, R. (2020). *Cyberweerbaarheid: risicobewustzijn en zelfbeschermend gedrag rondom cybercriminaliteit onder jongeren en mkb-ers.* Saxion Hogeschool. https://www.saxion.nl/binaries/content/assets/onderzoek/areas-living/maatschappelijke-veiligheid/saxion-haagse-hogeschool-cyberweerbaarheid.-risicobewustzijn-en-zelfbeschermend-gedrag-rondom-cybercrime-onder-jongeren-en-mkb-ers.pdf.

Ng, Z.X., Ahmad, A., Maynard, S.B., 2013. Information security management: factors that influence security investments in SMES. In: Proceedings of the 11th Australian Information Security Management Conference doi:10.4225/75/57b56667cd8e5.

Notté, R.J., Slot, L., van 't Hoff-de Goede, S. & Leukfeldt, E.R. (2019). *Cybersecurity in het mkb*. De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/cybersecurity-in-het-mkb_nulmeting_notte_et_al_2019.pdf?sfvrsn=4f0a5117_2.

Nurse, J.R., Creese, S., Goldsmith, M., Lamberts, K., 2011. Trustworthy and effective communication of cybersecurity risks: a review. In: Proceedings of International Workshop on Social-technical Aspects in Security and Trust. IEEE, pp. 60–68. doi:10.1109/STAST.2011.6059257.

Osborn, 2014. Business Versus technology: Sources of the Perceived Lack of Cyber Security in SMEs. Oxford University https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e.

Osborn, E., Simpson, A., 2018. Risk and the small-scale cyber security decision making dialogue—a UK case study. Comput. J. 61 (4), 472–495. doi:10.1093/comjnl/bxx093.

Rhee, H.S., Ryu, Y., Kim, C.T., 2005. I am fine but you are not: optimistic bias and illusion of control on information security. In: Proceedings of the 26th International Conference on Information Systems, pp. 381–394.

Rhee, H.S., Ryu, Y.U., Kim, C.T., 2012. Unrealistic optimism on information security management. Comput. Secur. 31 (2), 221–232. doi:10.1016/j.cose.2011.12.001.

Richardson, R., North, M.M., 2017. Ransomware: evolution, mitigation and prevention. Int. Manage. Rev. 13 (1), 10–21. https://digitalcommons.kennesaw.edu/facpubs/4276/.

Riek, M., Böhme, R., Moore, T., 2014. Understanding the influence of cybercrime risk on the e- service adoption of European Internet users. In: Proceedings of the Workshop on the Economics of Information Security.

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. J. Psychol. 91 (1), 93–114. doi:10.1080/00223980.1975.9915803.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo, J.T., Petty, & R.E. (Eds.), Social Psychophysiology: A Source Book. Guilford Press, pp. 153–176.

Rohn, E., Sabari, G., Leshem, G., 2016. Explaining small business InfoSec posture using social theories. Inform. Comput. Secur. 24 (5), 434–556. doi:10.1108/ICS-09-2015-0041.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur. 53, 65–78. doi:10.1016/j.cose.2015.05.012.

Sheeran, P., 2002. Intention—behavior relations: a conceptual and empirical review. Eur. Rev. Soc. Psychol. 12 (1), 1–36. doi:10.1080/14792772143000003.

Siponen, M., Mahmood, M.A., Pahnila, S., 2014. Employees' adherence to information security policies: an exploratory field study. Inform. Manage. 51 (2), 217–224. doi:10.1016/j.im.2013.08.006.

Spithoven, R., 2017. Keeping Trouble At a Safe distance. Unravelling the Significance of 'the fear of Crime'. Eleven International Publishing.

Spithoven, R., 2020. Verbonden risico's. Maatschappelijke veiligheid in De Black Box Society. Boom Criminologie.

Slovic, P., Finucane, M.L., Peters, E., MacGregor, D.G., 2004. Risk as analysis and risk as feelings: some thoughts about affect, reason, risk and rationality. Risk Anal. 24, 311–322. doi:10.1111/j.0272-4332.2004.00433.x.

Slovic, P., Peters, E., 2006. Risk perception and affect. Curr. Dir. Psychol. Sci. 15 (6), 322–325. doi:10.1111/j.1467-8721.2006.00461.x.

Sommestad, T., Karlzén, H., Hallberg, J., 2015. A meta-analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security and Privacy 9 (1), 26–46. doi:10.4018/IJISP.2015010102.

Sophos. (2022). The state of ransomware 2022. https://assets.sophos.com/X24WTUEQ/at/c5234fvn45pvmk5w6nhh4vkh/sophos-state-of-ransomware-2022-infographic.pdf.

Statistics Netherlands, 2020. MKB-statline. CBS https://mkbstatline.cbs.nl/#/MKB/nl/dataset/48038NED/table?ts=1619084773761.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J., Cotten, S.R., 2016. Understanding online safety behaviors: a protection motivation theory perspective. Comput. Secur. 59, 138–150. doi:10.1016/j.cose.2016.02.009.

Van 't Hoff-de Goede, S., van der Kleij, R., van de Weijer, S., Leukfeldt, R., 2019. Hoe Veilig Gedragen Wij Ons Online?. De Haagse Hogeschool https://www.researchgate.net/profile/Susanne-Van-t-Hoff-De-Goede/publication/354091450_Hoe_veilig_gedragen_wij_ons_online_Een_studie_naar_de_samenhang_tussen_kennis_gelegenheid_motivatie_en_online_gedrag_van_Nederlanders/links/6124e1d2169a1a0103205726/Hoe-veilig-gedragen-wij-ons-online-Een-studie-naar-de-samenhang-tussen-kennis-gelegenheid-motivatie-en-online-gedrag-van-Nederlanders.pdf.

Van den Berg, B., Keymolen, E., 2017. Regulating security on the Internet: control versus trust. Int. Rev. Law Comput. Technol. 31 (2), 188–205. doi:10.1080/13600869.2017.1298504.

Van der Kleij, R., de Bruin, I., van 't Hoff-de Goede, S., Leukfeldt, E.R., 2019. Pilotonderzoek Cyberweerbaarheid Mkb-Retailers in De Regio Den Haag. De Haagse Hogeschool https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/cyberweerbaarheid-mkb-retailers.pdf?sfvrsn=49327266_0.

Van der Kleij, R., Leukfeldt, R., 2019. Cyber resilient behavior: integrating human behavioral models and resilience engineering capabilities into cyber security. In:

International Conference on Applied Human Factors and Ergonomics, pp. 16–27. doi:10.1007/978-3-030-20488-4_2.

Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: insights from habit and protection motivation theory. Inform. Manage. 49 (3–4), 190–198. doi:10.1016/j.im.2012.04.002.

Veenstra, S., Zuurveen, R., Stol, W., 2015. Cybercrime Onder bedrijven: Een onderzoek Naar Slachtofferschap Van Cybercrime Onder Het Midden-En Kleinbedrijf En Zelfstandigen Zonder Personeel in Nederland. Cybersafety Research Group https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf.

Webb, T.L., Sheeran, P., 2006. Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. Psychol. Bull. 132 (2), 249–268. doi:10.1037/0033-2909.132.2.249.

Wilson, M., McDonald, S., Button, D., McGarry, K., 2022. It Won't happen to me: surveying sme attitudes to cyber-security. J. Comput. Inform. Syst doi:10.1080/08874417.2022.2067791.

Witte, K., 1992. Putting the fear back into fear appeals: The extended parallel process model. Communications Monographs 59 (4), 329–349. doi:10.1080/03637759209376276.

Luuk Bekkers: Luuk Bekkers is a PhD-candidate at the center of Expertise Cyber Security of THUAS and has a master's degree in criminology and psychology. His research focusses primarily on money mules, in which he takes both a qualitative and quantitative approach in order to explain the involvement of individuals into cybercrime. Luuk also explores other topics related to the human factor of cybercrime.

Susanne van 't Hoff-de Goede: Susanne van 't Hoff-de Goede is a criminologist and postdoc researcher. Her research interest go out to explaining, preventing and integrally tackling crime. At the center of Expertise Cyber Security (The Hague University of Applied Sciences in The Netherlands), she studies the human factor in cybercrime: offenders, victims and law enforcement. Her research focusses, amongst other things, on cybervictimization and interventions aimed at reducing cybercrime.

Ellen Misana-ter Huurne: Ellen Misana-ter Huurne is a senior researcher at the Public Security research group at Saxion University of Applied Sciences. Ellen holds a Master's Degree in Communication Studies and a Ph.D. in Behavioral Sciences. Her main research interests include risk communication and public responses to risks. More specifically, she focuses on how people respond to risk information and how risk-related self-protectieve behaviors can be stimulated through risk communication interventions.

Ynze van Houten: Ynze van Houten is a Senior Researcher at the research group Public Security at Saxion University of Applied Sciences. He studied Experimental Psychology, has a PhD in Behavioral Sciences, and has specialized in the human interaction with technology. His-current research focuses on how to increase the resilience of different target groups against different types of cybercrime.

Remco Spithoven: Remco Spithoven is head of the research group of Public Security at Saxion University of Applied Sciences. After his master of Public Administration with a specialization in security studies and his PhD in the Social Sciences with a research focus on fear of crime, his research focusses on risk perception, cyber resilience and digital security. He is editor in chief of "Tijdschrift voor Veiligheid" (Dutch, scientific) and "Basisboek integrale veiligheid" (Dutch, applied sciences).

Rutger Leukfeldt: Rutger Leukfeldt is a Senior researcher at the NSCR and director of the center of Expertise Cybersecurity of THUAS. Rutger has been doing research into the human factor of cybercrime for 15 years. During that period, he was involved in both fundamental academic research and applied research for companies and governments. Rutger carries out both quantitative and qualitative studies, but his expertise lies in qualitative methods. Over the years, he analyzed numerous large scale police investigations and interviewed both cybercriminals and victims.