The Impact of Threat and Efficacy on Information Security Behavior: Applying an Extended Parallel Process Model to the Fear of Ransomware

Kristin Masuch
University of Goettingen
kristin.masuch@uni-goettingen.de

Sebastian Hengstler
University of Goettingen
s.hengstler@stud.uni-goettingen.de

Laura Schulze
University of Goettingen
laura.schulze@uni-goettingen.de

Simon Trang
University of Goettingen
strang@uni-goettingen.de

Abstract

Information security has become an increasingly important aspect in companies and households during this time of digitalization. Cyber attacks and especially ransomware attacks are a growing threat. How people react to and perceive this threat is a central component of this study. This paper is meant to investigate how threat and efficacy influence individuals' information security behavior. For this purpose, a structural equation model was developed using the Extended Parallel Process Model (EPPM). The results show that participants who received a low threat message in their ransom demand were less afraid and more likely to deal with the issue. At the same time, they were not as confident as people who perceived a significant threat. Participants who felt that they had little adequate protection against ransomware were more fearful and therefore dealt with the topic more defensively. Conversely, they also had the intention to behave safely.

1. Introduction

Information technology is being used both professionally and privately, so the danger of security attacks is omnipresent [1]. This study examines the extent to which individuals can be motivated to protect their data and prevent attacks. Some of such attacks, called fear appeals, involve persuasive messages, which include plausible threats. These fear appeals are mainly used in the healthcare industry [2]. In the relevant academic literature, fear appeals are often used to describe negative consequences and thus reduce undesired behavior [2]. The use of fear appeals is widespread in research, and such messages are widely believed to be more effective achieving a security threat [2], [3]. The German Federal Office for Information Security assumes that severe threats are mostly posed by ransomware attacks, which cost 8 billion dollars worldwide in 2017 [4]. One of the most well known ransomware types is WannaCry, which caused enormous global damage estimated at several hundred million to four billion dollars [4]. WannaCry attacked more than 200,000 computers in 150 countries [4]. Such ransomware attacks can lead to, among other things, data loss due to access by third parties [5]. Users can be motivated to protect their data from such attacks to mitigate ransomware threats and ensure information security behavior. Two common methods to encourage users to increase their data security and be less afraid of ransomware attacks are creating backups and using antivirus scanners [5]. However, past research in the field of information security compliance behavior shows that technical measures alone are not sufficient to guarantee information security. Primarily because security attacks are mainly targeted at the weakest link in the security chain, it is even more important to take a socio-technical approach and implement behavioral measures to minimize individuals' non-secure behavior [6].

The literature on information security compliance behavior research often used and defined fear appeal as follows: When a person is confronted with such threats, assessment mechanisms are triggered, leading to certain behavior in the given situation and deciding whether the person protects their security. One theory that explains the influence of these messages is Witte's [7] Extended Parallel Process Model (EPPM), which is often used in health-related contexts [7]–[10]. The EPPM includes components of other established approaches for explaining such behavior-oriented decision-making processes, such as the Protection Motivation Theory (PMT) [11]–[13] and the fear control framework, according to Leventhal [14]. The EPPM is intended to prevent the protection or

URI: https://hdl.handle.net/10125/71423
978-0-9981331-4-0

defensive motivation process from being considered alone in the PMT or the fear control framework and provides a more holistic view on the decision-making process [15].

Looking at the context of the behavior-specific effects of ransomware on individuals, no explanations that describe the behavior of individuals when confronted with ransomware can be identified so far. Although there are technical measures to avoid ransomware, approaches to avoid the effectiveness of ransomware from a social-behavioral perspective, which aims to increase awareness and behavior towards a security threat through ransomware, are still missing. This paper aims to contribute to an explanation of the problem and examines the following research question:

RQ: *How do fear appeals influence users' intentions to change their information security behaviors in ransomware?*

Our findings yield important insights for theory and practice. From a theoretical point of view, we provide the first approach to explain ransomware security behavior and provide a starting point for further theoretical consideration of one of the most current and dangerous security risks. The EPPM model lends itself to our approach, because it uses well-known constructs to explain threat and coping appraisals and associates them in context with both behavioral intention and defensive avoidance. Although current information security research focuses on the connection between threat, coping appraisals and behavioral intention, a connection with fear and defensive avoidance in a unified context and model is missing [6], [9]. Additionally, practitioners, such as information security managers, can use our results to develop measures against ransomware's effectiveness and meet the need for socio-technical measures in this area. Private individuals receive advice from our results on how they can better protect themselves against ransomware.

We investigated the stated question by implementing an empirical research design based on an EPPM model adapted for our context. We collected data from a sample of 507 German participants to analyze our research model using Partial Least Squares (PLS) structural equation modeling.

The remainder of the paper is structured as follows. After the introduction, the theoretical foundation is explained in chapter two. Afterward, we provide an overview of the EPPM. Next, our hypotheses and the research model are introduced in chapter three. After explaining our methodology in chapter four, the structural model and measurement of this study are presented in chapter five. This is followed by evaluating the results and the subsequent discussion in chapter six, which includes implications and limitations. We conclude our study in chapter seven.

2. Theoretical background

The following section outlines the relevant theoretical foundation for the study. First, fear appeal and the extended parallel process model are explained. Next, the practical context is described, declaring ransomware as an information security threat.

2.1. Fear appeal and the extended parallel process model

In a basic definition, fear appeals can be described as convincing messages aimed at frightening people. This is to be achieved by describing the terrible things that will happen to a person if they act contrary to the message sent by the fear appeal [16]. A fear appeal message is intended to get a person to change their behavior because of fear. Fear appeals generally consist of three elements: Fear, threat, and effectiveness. The result of a fear appeal is the acceptance of a message, which is defined as a change of attitude, intention, or behavior [12]. Fear appeal is relevant in our context because it initiates message transmission and is the trigger for consideration and causes a specific behavior. In this context, a threat represents an external stimulus that exists independently of an individual's perception. If an individual perceives the threat, it can be said that the individual is aware of a threat. When a fear appeal is constructed, it is designed to convey first that there is a threat to an individual, and second, to show its severity and the vulnerability of the individual to the threat. From the fear appeal, the considered individual should derive the threat severity and the perceived vulnerability to the threat. In the considered behavioral formation process, as soon as a person is aware of a threat, the convictions about the severity of the threat and the probability of personally experiencing the threat also build up. In addition to a threat, the individuals' efficacy also influences the behavioral development process, triggered by a fear appeal [12].

The construct efficacy can be distinguished between response efficacy and self-efficacy [16]. Response efficacy is the extent to which a person believes a measure is effective against a threat. If a person does not believe a measure to be successful, they are less willing to adopt a behavior against it [17]. Self-efficacy is the degree to which a person believes in their ability to perform an action against a threat

[11]. The term self-efficacy thus refers to a person's perceived competence. In information security, people with a high degree of self-efficacy are more willing to implement security measures [17].

Various approaches describe the relationships between fear appeal, efficacy, and threat and their dependence on behavior formation in the existing literature. One of the models is the PMT by Rogers [18]. The PMT is divided into three phases [19]. In the first phase, information is obtained related to fear appeal and experiences with the danger. The second phase is the cognitive mediating process. This process is divided into two components: Threat assessment and coping assessment [19]. The last phase is coping, in which the behavioral intention is examined [19]. The advantage of PMT is that it is a widely used model among researchers for the influence of anxiety attacks [11]. Another model is the Parallel Response Model [14]. In this model, it is assumed that communication causes fear on the one hand and persuasion on the other hand. It should be noted that fear does not generate persuasive power. The theory focuses on the factors that lead to mastery of the information process, such as behavior that causes fear [14]. In addition, with its fear and coping reactions, one's organism can also serve as information that influences individual decisions [14]. Different sources of information can, therefore, provoke particular behavior patterns at certain times [14].

An extended model for explaining fear appeals and their impact on behavior is the EPPM. The model describes a combination of the danger control/fear control framework of Leventhal [14] with some elements of Rogers' [18], [19] original PMT [16]. These are subdivided into self-efficacy, response efficacy, susceptibility, and severity. These components are perceived and evaluated by the recipient. Self-efficacy describes the expectation of a person to carry out desired actions successfully based on their competencies, while response effectiveness refers to a person's beliefs about whether or not an action actually averts a threat. Susceptibility refers to the subjective perception of a risk for a perceived threat's negative impact, while severity describes the perceived threat's severity. Depending on the degree of perceived efficacy and perceived threat, there are several possible outcomes. If the perceived threat and perceived self-efficacy are high, this leads to protection motivation and adaptive changes. This process is called threat control [16]. When the threat is high, but the response efficacy to the threat is low, the message leads to anxiety control processes that cause maladaptive changes. If the threat is low, there is no response because no fear has been generated. According to the EPPM model, the higher the threat, the greater the evoked fear, the more attention the message attracts, and the more the message is integrated into the behavioral education process [16]. The process is as follows. First, the message and the threat are evaluated. If the resulting fear is high, the individuals' efficacy is also evaluated. The fear control process and the threat control process run simultaneously. The threat is not the decisive variable, rather the threat's efficacy, since it determines which process will be dominant [16]. Threat control processes are processes in which the individual manages the threat by taking preventive measures to reduce an event's probability. In contrast, fear control processes are primarily emotional processes in which the individual only copes with their fear rather than with the danger [16]. In our study's framework, we use the EPPM model, because it considers both protective and maladaptive coping mechanisms compared to PMT and the hazard control/anxiety control framework, and thus describes the effects on fear appeals in a holistic way. A maladaptive coping mechanism, also called defensive avoidance, describes how to avoid dealing with a stressor.

2.2 Ransomware as an information security threat

According to relevant practice related literature, ransomware is defined as follows: Ransomware describes malware that restricts or prevents access to data and systems and releases these resources only against payment of a ransom. The name ransomware is a nested word from the terms "ransom" and "malware"." [5]

Ransomware enables third parties to block or prevent system access or encrypt user data. Windows systems are most often affected. The most common attack vectors are attachments of spam emails and "drive-by-attacks" using exploit kits (i.e., malware on websites), USB sticks, and network drives [20]. According to a BSI survey, ⅓ of the companies surveyed said they had been affected by at least one ransomware incident in the last six months, with ¾ of cases involving email attachments. The consequences of ransomware, both in the private and business sector, can be seen primarily in damage to the own reputation, the loss of data and hardware, as well as monetary damages [5]. Protection measures in organizations include backing up relevant data, raising employees' awareness of current attack methods (e.g., macros in Microsoft Office documents), and using antivirus scanners [21].

Existing research on information security behavior does not yet consider ransomware, which leaves open

potential for identifying socio-technical measures to ensure information security regarding ransomware.

3. Research model and hypotheses development

The following research model (Figure 2) is based on the EPPM [16] and the implementation of the work of Birmingham et al. [8]. We adapted the model for our research context of information security. The threat construct consists of the mechanisms susceptibility and severity, and the construct efficacy can be further sub-conceptualized into self-efficacy and response-efficacy. We adapted the original constructs fear and defensive avoidance and adapted the original construct intention into behavioral intention related to ransomware.

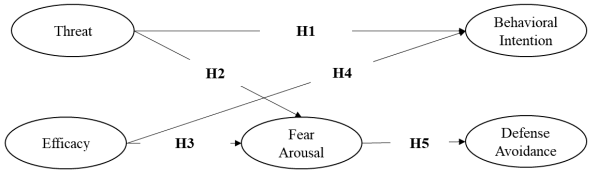

Figure 1. Research Model

Based on Witte's EPPM [16], we propose the following five hypotheses.

As can be inferred from the EPPM [16], we aggregate threat susceptibility and threat severity in one measuring construct. Despite the dependence on efficacy, regardless of whether the danger control process or the fear control process initiates, the level of perceived threat has, in both cases, an essential influence on the intention to protect one's security. The perceived threat has an essential influence because of the danger control process; in our case, intention to take protective action only initiates when the threat is sufficiently severe [16]. To ensure that participants are offered an incentive to protect themselves from ransomware, ransomware dangers are emphasized in the case of a fear appeal with a high threat. Thus, we suggest the following hypothesis:

H1: *Threat has a positive effect on behavioral intention.*

In contrast to the PMT, the EPPM considers fear as another variable [16]. The danger control process or fear control process is initiated based on the fear appeal's efficacy. Efficacy should be low if threat influences fear arousal. Nonetheless, fear cannot be evoked if the threat condition is low, so a more threatening fear appeal positively influences fear [16]. By illustrating the danger of ransomware, depending on the degree of efficacy, fear can be aroused. With this understanding, we propose the following hypothesis:

H2: *Threat has a positive effect on fear arousal.*

The construct efficacy consists of two components, self-efficacy and response efficacy [16]. The EPPM shows that only efficacy determines whether the danger control process or fear control process occurs [16]. In precise terms, fear arousal increases when efficacy is low in the fear control process [7]. One explanation is that people might feel helpless or incapable of opposing the threat [7], [22]. Therefore, fear arousal is partly influenced by security technologies' level of security [13]. If people assume that antivirus scanners and backups are not effective against ransomware, fear arousal increases. Therefore, we propose the following hypothesis:

H3: *Efficacy has a negative effect on fear arousal.*

In contrast to increased fear arousal due to lower efficacy, fear appeals with high efficacy positively influence intentions to behave securely if they are sufficiently threatening. This hypothesis is supported by Witte's research on AIDS prevention [7]. Thus, the danger control process initiates. Anderson and Agarwal [23] indirectly support this hypothesis; they found a significant positive effect on attitude, which also significantly influences intention. An explanation could be that there is a realistic possibility for a person to oppose or prevent the threat if the danger is significant enough to merit protection [16], [22]. More specifically, this means that people are willing to oppose a potential ransomware threat if the defense measures are effective against it to protect themselves. The individuals must also be confident that they can protect themselves, as demonstrated by the ease of use of protective measures with high efficacy in the fear appeals [13]; therefore, we derive the following hypothesis:

H4: *Efficacy has a positive effect on behavioral intention.*

Fear can be described as an inner emotional reaction with psychological and physiological dimensions triggered by cognitive stimuli [22]. Fear has been hypothesized to be aroused by fear appeals with high threat and low efficacy. Fear was found to have a significant positive effect on avoidance [24]. Hence, fear is referred to as a driver [14]. When transferred to the EPPM, the fear control response follows the fear control process' initiation [22]. Defensive avoidance is denying or blocking confrontation with the threat [7], [24]. This defensive avoidance can reduce the feeling of discomfort [24]. To reduce the uncomfortable feelings, individuals will

avoid information about the potential dangers of ransomware, in case of a positive influence of fear on defensive avoidance. Contrarily, Birmingham et al. [8], who also examined fear appeals in a health-related context, demonstrated that fear has a significant negative effect on defensive avoidance. Despite the contradictory results of the influence of fear on defensive avoidance, we offer the following hypothesis:

H5: *Fear arousal has a positive effect on defensive avoidance.*

4. Methodology

An intervention design using two independent variables was developed to test the proposed hypotheses in an online survey. The independent variables were manipulated and randomly assigned to the participants [25]. In the following sections, we describe the data collection of the sample and the research design, and the measurement of the variables.

4.1 Research design

To test our hypotheses, we manipulated the independent variables to correspond to the following conditions: high vs. low threat and high vs. low efficacy. It is important to note that the participants always received a message that expresses threat in combination with a message that expresses efficacy. The following possible combinations were shown to the participants by means of randomization: high threat/ high efficacy (HT/HE), high threat/ low efficacy (HT/LE), low threat/ high efficacy (LT/HE), and low threat/ low efficacy (LT/LE). The information that was displayed to the participants in the survey is shown in Table 1.

Table 1. Intervention messages

Low Threat	*Attacks by ransomware like WannaCry can cause economic damage. Ransomware is malicious software that restricts or prevents access to data and systems and only releases them against a ransom payment. The damaged parties can, therefore, be deprived of data. Ransomware attacks account for only 7% of all malware attacks worldwide. In addition, a sharp decline in ransomware attacks has been observed since 2018.*
High Threat	*Attacks by ransomware like WannaCry have caused economic damage of more than eight billion dollars worldwide in 2017. This damage amounts to millions in Germany itself. Ransomware is the term used to describe malware that restricts or prevents access to data and systems and only releases them against a ransom payment. The damaged parties can, therefore, be deprived of essential data. The formation of new types of ransomware can lead to new methods of attack. Therefore, there is no reason to sound the all-clear regarding ransomware attacks.*
Low Efficacy	*Possible measures effective against other malware, such as regular updates or the use of antivirus programs, are not always sufficient against ransomware. 86% of ransomware could not be detected by the standard antivirus program (Windows Defender) in a simulation test. Ransomware attacks can block access to the backups of data (backup copies). Due to new possibilities to smuggle ransomware into the system, it is harder or even impossible for antivirus programs to detect it.*
High Efficacy	*Essential to protect oneself from ransomware attacks is antivirus programs, as they have a detection rate of up to 96%. Antivirus programs are designed to prevent malicious programs from running on the computer. The Federal Office for Information Security also expressly recommends preventive measures such as regular updates and backups of data (backup copies). In just under 7 out of 10 cases, the data blocked by ransomware can be made accessible again through backups. The measures mentioned above can be implemented quickly and easily.*

The low threat condition was designed to convince participants that the threat was trivial [15], i.e., that ransomware was not a severe threat. Contrarily, the high threat condition convinced the participants that they were at significant risk due to the ransomware's omnipresent danger. In the low efficacy condition, we based our manipulation on the assertion that a threat cannot be averted [15], i.e., measures against ransomware are ineffective. In the high efficacy condition, we manipulated efficacy, so participants believed that they could effectively avert a threat, so measures against ransomware are successful [15]. All four intervention messages were approximately the same length.

4.2 Data collection and sample

We collected data among participants through an online survey. The participants consisted of people who work with a computer in their daily work (or private) lives. The questionnaire was translated from English into German in order to ensure comprehensibility for the participants. An overview of the English questions is provided in the appendix. In addition to the intervention messages that describe threat and efficacy, manipulation checks were carried out, and we included questions on three constructs relevant to our study context. Participants were introduced to the scenario, after which we included attention checks to make sure the participants read and understood the intervention message. The behavioral intention (BI) scale we used is based on the research of Johnston and Warkentin [11], Workman et al. [26], and Ng et al. [27]. The defensive avoidance (DA) and fear arousal (FEAR) items were adapted from Birmingham et al. [8]. The questions were adapted to the context of ransomware. Additional variables we collected include Johnston and Warkentin's [11] general questions on information security and demographic questions. We used a five-point Likert scale to measure our items. Last, we ensured that the participants were debriefed about ransomware's real danger and the possibility to oppose it. The debriefing was executed through a text, which contained all information on efficacy and threat, in contrast to the partial information in the intervention messages. Furthermore, we conducted a preliminary study with 12 subjects (8 complete responses) to check our questionnaire's consistency and make sure that the participants perceive the right levels of threat and efficacy in the questionnaire.

578 German participants took part in our study that we ran from July to August 2019. Among these answers, 507 were complete and valid answers, which were used for the evaluation. Of these, 58.6% were female, 40.4% male, and 1% other. The average age of the participants was 25.6 years. Most participants hold a bachelor's degree (37.9%) or completed high school (32.4%). Furthermore, most participants were young professionals with 1-2 years of work experience (25.4%). This implies that our participants are subject to threats by ransomware in corporate and/or private settings. The distribution of the participants across the four groups was approximately equal (HT/HE: n= 122, HT/LE: n = 130, LT/HE: n = 124, LT/LE: n = 131).

5. Data analysis and results

A Structural Equation Modeling (SEM) approach was used to evaluate the data. It allows testing and evaluating hypothesis-based causal relationships [28]. Information systems, as well as several other research disciplines have applied the variant-based Partial Least Square (PLS) method. The SEM technique is also particularly well suited for the current research, as it allows multiple relationships between latent variables to be measured with multiple indicators [29]. Moreover, the paths for measuring the latent variables and the hypothetical relationships between the latent variables can be estimated simultaneously.

5.1. Measurement validation

There are two independent variables for the model to be examined: threat and efficacy. These independent variables are manipulated in the study and are, therefore, binary variables (0 or 1). In addition, reflective relationships of the variables fear, behavioral intention, and defense avoidance were modeled. It was found that all elements load and internal consistencies of the reflectively modeled constructs are above the limit of 0.7. The only exclusions are the second and third elements of the defense avoidance construct (see appendix). These were removed due to the limit of 0.7 not being reached. The criteria of composite reliability (CR) and extracted mean variance (AVE) are shown in table 2. They are used to assess the reliability and validity of the construct. The requirements are met if all constructs evaluate CR values higher than 0.7, and AVE values higher than 0.5 [30]. The requirements for both criteria are met because all CR values are well above the limit of 0.7, while all AVE values also reach the limit of 0.5. By comparing the AVE's square root with the correlations between the constructs, Fornell and Larcker offer an approach to assess discriminatory validity. The comparison shows that all constructs retain a higher value for the AVE's square root than for the correlation with other constructs [31].

Table 2. Construct validation

	AVE	CR	EF	TA	FEAR	BI	DA
EF	n.a.	n.a.	1				
TA	n.a.	n.a.	-.002	1			
FEAR	.780	.946	-.126	.162	.883		
BI	.702	.934	.130	.163	.212	.838	
DA	.674	.796	-.026	-.042	.316	-.020	.821

EF = Efficacy; TA = Threat; FEAR = Fear Arousal, BI = Behavioral Intention; DA = Defense Avoidance

5.2 Hypotheses testing

The PLS method was used for estimation to test the theoretical structural model described above. A 5000-sample bootstrapping resampling method was used to assess the significance of the paths. The estimation of the path model is shown in figure 2 for the relevant paths. From these results, it can be concluded that we find support for the basic structure of the theory.

A significant effect was found for all hypotheses. It was found that threat (.163; significant at .01) has a significant positive effect and efficacy (.126; significant at .01) has a significant negative effect on fear. In turn, fear has a significant positive effect on defense avoidance (.319; significant at .01). A significant positive effect of threat (.163; significant at .01) and efficacy (.131; significant at .01) on behavioral intention was also observed.

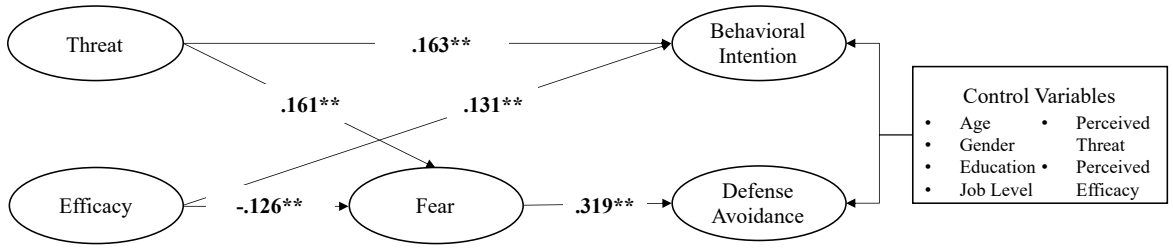

Figure 2. Structural model with path coefficients

*Note: ** significant at .01*

Additionally, the following control variables were used: age, gender, educational level, job level, threat, and efficacy. Except for threat on defense avoidance (-.091 significant at .01), these control variables had no significant influence. In summary, all proposed hypotheses are supported.

6. Discussion and summary of findings

The following is a summary of the results. Moreover, the implications for theory and practice are reviewed. Afterward, the limitations of the work and possibilities for future research are discussed.

6.1. Summary of findings

The paper examines how the EPPM with its constructs threat and efficacy in ransomware can be used to influence fear and thereby, defense avoidance and the behavioral intention to behave securely. Thus, an understanding of how the EPPM works in the context of ransomware and whether it is applicable is developed. It can be summarized that threat and efficacy positively influence behavioral intention, i.e., participants who have been positively influenced by these two constructs tend to behave more securely. Contrarily, the positive effect of threat and the negative effect of efficacy on fear result in defensive avoidance, i.e. participants tend take no action. In summary, one can say that this is a current and highly relevant topic with high practical relevance. The effects of the EPPM have already been investigated in various contexts, but have never been investigated in the context of ransomware. Therefore, this paper presents both theoretical and practical implications. However, this paper is not free of limitations, which, at the same time, provide opportunities for future research.

6.2. Implications for theory and contributions to literature

This study provides a theoretical contribution by testing the EPPM in the context of ransomware. This should lead to a better understanding of how the EPPM works in the new context. The EPPM was shown through Witte [7] to influence fear, defense avoidance, and behavioral intention [25]. Our results suggest that some of the suggestions of the EPPM from different use cases can be transferred to information security and especially to ransomware. One of these arguments is that fear attacks with high threat levels lead to a higher fear level. The fear of ransom demands is increasing. Additionally, a higher threat also leads to a higher intention to change behavior positively. Therefore, it is also an incentive for individuals to

protect themselves from ransom demands. This positive change is also called acceptance of the message [7]. Constructive effectiveness also leads to a higher intention to change behavior, as Witte [7] proposed. Besides, we found that efficacy's effect on fear is negative, matching Witte's research [16]. In comparison with existing information security literature, similar results can be seen. In our work, we found similar effects for the influence of threat and efficiency on behavioral intention, like Vance et al. [32]. However, in contrast to other research, we found significant effects between susceptibility, severity, self-efficacy and behavioral intention in our EPPM model, in contrast to the model of Menard et al [33]. Furthermore, effectiveness has a strong influence on the intention to implement information security measures. People are willing to take security measures, such as saving backups and using antivirus scanners. This suggests that people will be more concerned about their data security and are confident that they can do so. It will allow us to expand the existing literature on the EPPM and its impact. This could be achieved by investigating, through experimental research, how behavioral intention, fear, and thus defense avoidance can be influenced in the case of ransomware, complementing the existing security literature. It can illustrate how further research can explain the constructs threat and efficacy, such as helping companies define communication strategies for data security. It is also essential that research and practice address the problem, as ransomware is becoming an increasingly relevant issue, threatening companies and individuals [17]. Moreover, both companies and private individuals incur unplanned costs after a ransomware attack, which could be reduced by appropriate practices [34].

6.3. Implications for practice

The results identified have practical relevance in addition to the theoretical contribution. For example, they can help companies optimize their future corporate communication strategies regarding the danger of ransomware. Companies can use our findings to adapt their communication so that the best possible results can be achieved even in the case of a ransomware attack. The results can also provide insights into how private individuals can be influenced and warned about ransomware and how threat and efficacy can influence people's fear and behavior. As already mentioned, ransomware attacks can have fatal consequences. Therefore, it is vital to investigate how the consequences of ransomware attacks can be reduced or even prevented. Our study's results suggest that by using a statement that conveys a high threat, people have a higher intention to behave securely and are more afraid of a ransomware attack, which leads to a defensive attitude. If, however, the statement that there are effective ways to protect themselves from the threat is also included, the participants tend to have a higher intention to behave securely again, and the fear of the threat can be reduced, which leads to a less defensive attitude. Accordingly, statements about ransomware that are intended to reduce the danger should always contain both aspects. This means that individuals can tackle a high threat, in case they know that there are effective mechanisms to protect oneself from the threat of ransomware.

6.4. Limitations and future research

While our study yields important findings in information security behavior, there are some limitations we would like to address in the following. Whereas information security is a concern to a broad spectrum of the population, our results are based on 507 German participants, who have varying levels of professional experience. Compared to other countries, Germans seem to be more aware of cybercrime than other Europeans [34] are. Therefore, considering cultural differences might be insightful in future research. We chose ransomware as a relevant instantiation of information security threats and its appeal to individuals' efficacy because of its prevalence [4]. However, ransomware is just one variant of malware, including spyware, phishing, botnets, worm-based attacks, or surveillance attacks [35]. Additionally, specific information security behaviors could be investigated. Some examples of this are log-off/lock screen behavior [36] and the opening of email attachments [37]. While we build on the advantages of a controlled setting, in which we were able to manipulate the amount of threat and efficacy participants were exposed to, future research could study actual user behavior.

7. Conclusion

This study deals with ransomware statements' influence on people's fear and behavior using the EPPM. By formulating a research design that varies the levels of the constructs threat and efficacy, 507 study participants were interviewed. The data set was evaluated using a structural equation model. This study's results provide valuable insights into how fear appeals in the form of threat and efficacy affect the fear and behavior of individuals who may be endangered by ransomware. The study shows that the participants who were given a low threat message in

their ransomware statement were less afraid and more likely to deal with the issue. At the same time, they were not as secure as people who had perceived a significant threat. In addition, participants who felt that they had little practical protection against ransomware were more afraid and therefore tended to be more defensive about the topic. However, they simultaneously had the intention to behave securely. In summary, it can be stated that the processes of the EPPM help explaining individuals' reactions when facing the danger of ransomware.

8. References

[1] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance," Journal of the Association for Information Systems, vol. 19, 2018, pp. 689–715.

[2] N. Rhodes, "Fear-Appeal Messages: Message Processing and Affective Attitudes," Communication Research, vol. 44, no. 7, 2017, pp. 952–975.

[3] K. Witte and M. Allen, "A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns," Health Educ Behav, vol. 27, no. 5, 2000, pp. 591–615.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Die Lage der IT-Sicherheit in Deutschland 2018," Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018. https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (accessed Jul. 12, 2020).

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI), Ed., "Lagedossier Ransomware." 2016.

[6] A. Vance, M. Siponen, and S. Pahnila, "Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory," Information & Management, vol. 49, no. 3–4, 2012, pp. 190–198.

[7] K. Witte, "Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM)," Communication Monographs, vol. 61, no. 2, 1994, pp. 113–134.

[8] W. C. Birmingham et al., "Effectiveness of the Extended Parallel Process Model in Promoting Colorectal Cancer Screening," Psycho-Oncology, vol. 24, no. 10, 2015, pp. 1265–1278.

[9] N. Carcioppolo, J. D. Jensen, S. R. Wilson, W. B. Collins, M. Carrion, and G. Linnemeier, "Examining HPV Threat-to-Efficacy Ratios in the Extended Parallel Process Model," Health Communication, vol. 28, no. 1, 2013, pp. 20–28.

[10] E. K. Maloney, M. K. Lapinski, and K. Witte, "Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model," Social and Personality Psychology Compass, vol. 5, no. 4, 2011, pp. 206–219.

[11] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," MIS Quarterly, vol. 34, no. 3, 2010, pp. 549–566.

[12] J. Ophoff and M. Lakay, "Mitigating the Ransomware Threat: A Protection Motivation Theory Approach," in International Information Security Conference Proceedings, Cham, 2019, vol. 973, pp. 163–175.

[13] C. Yoon, J.-W. Hwang, and R. Kim, "Exploring Factors That Influence Students' Behaviors in Information Security," Journal of Information Systems Education, vol. 23, no. 4, 2012, pp. 407–415.

[14] H. Leventhal, "Findings and Theory in the Study of Fear Communications " Advances in Experimental Social Psychology, vol. 5, 1970, pp. 119–186.

[15] L. Popova, "The Extended Parallel Process Model: Illuminating the Gaps in Research," Health Educ Behav, vol. 39, no. 4, 2012, pp. 455–473.

[16] K. Witte, "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," Communication Monographs, vol. 59, no. 4, 1992, pp. 329–349.

[17] J. M. Blythe, L. Coventry, and L. Little, "Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors," 2015 Symposium on Usable Privacy and Security, 2015, pp. 103–122.

[18] R. W. Rogers, "A Protection Motivation Theory of Fear Appeals and Attitude Change," Journal of Psychology; Provincetown, Mass., etc., vol. 91, no. 1, 1975, pp. 93-114.

[19] R. W. Rogers, "Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," Social Psychophysiology: A Sourcebook, 1983, pp. 153–176.

[20] A. Zimba and M. Chishimba, "Understanding the Evolution of Ransomware: Paradigm Shifts in Attack Structures," International Journal of Computer Network and Information Security, vol. 11, no. 1, 2019, pp. 26–39.

[21] J. M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and Effectiveness of Organizational Information Security Measures," Information Management & Computer Security, vol. 16, no. 4, 2008, pp. 377–397.

[22] K. Witte, "Chapter 16 - Fear as Motivator, Fear as Inhibitor: Using the Extended Parallel Process Model to Explain Fear Appeal Successes and Failures," in Handbook of Communication and Emotion, P. A. Andersen and L. K. Guerrero, Eds. San Diego: Academic Press, 1996, pp. 423–450.

[23] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," MIS Quarterly, vol. 34, no. 3, 2010, pp. 613–643.

[24] P. A. Rippetoe and R. W. Rogers, "Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat," Journal of Personality and Social Psychology, vol. 52, no. 3, 1987, pp. 596–604.

[25] C. Atzmüller and P. M. Steiner, "Experimental Vignette Studies in Survey Research," Methodology, vol. 6, no. 3,2010, pp. 128–138.
[26] M. Workman, W. H. Bommer, and D. Straub, "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," Computers in Human Behavior, vol. 24, no. 6, 2008, pp. 2799–2816.
[27] B.-Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective," Decision Support Systems, vol. 46, no. 4, 2009, pp. 815–825.
[28] J. F. Hair, M. Sarstedt, C. M. Ringle, and J. A. Mena, "An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research," Journal of the Academy of Marketing Science, vol. 40, no. 3, 2012, pp. 414–433.
[29] V. E. Vinzi, L. Trinchera, and S. Amato, "PLS Path Modeling: From Foundations to Recent Developments and Open Issues for Model Assessment and Improvement," in Handbook of PLS and Marketing, vol. 40, W. W. Chin, V. E. Vinzi, J. Henseler, and H. Wang, Eds. 2006, pp. 47–82.
[30] R. R. Bagozzi and Y. Yi, "On the Evaluation of Structural Equation Models," Journal of the Academy of Marketing Science, 2988, pp. 74–94.
[31] C. Fornell and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error," Journal of Marketing Research, vol. 18, no. 1, 1981, pp. 39–50.
[32] Vance, A., Siponen, M., Pahnila, S.: "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory." Information & Management. 49, 190–198 (2012).
[33] Menard, P., Bott, G.J., Crossler, R.E.: "User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory." Journal of Management Information Systems. 34, 1203–1230 (2017).
[34] European Commission, "Europeans' Attitudes Towards Cyber Security," Special Eurobarometer 499, 2020.
[35] D. He, S. Chan, and M. Guizani, "Mobile Application Security: Malware Threats and Defenses," IEEE Wireless Communications, vol. 22, no. 1, 2015, pp. 138–144.
[36] M. Warkentin and R. Willison, "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," European Journal of Information Systems, vol. 18, no. 2, 2009, pp. 101–105.
[37] K.-P. Yee, "Aligning Security and Usability," IEEE Security Privacy, vol. 2, no. 5, 2004, pp. 48–55.

9. Appendix

Table 3. Operationalization of constructs

Fear Arousal [8]	
I get very scared when I think that I might be affected by ransomware.	FEAR1
When thinking about being affected by ransomware, I get very worried.	FEAR2
I feel bad just thinking about the possibility of being affected by ransomware.	FEAR3
When I think about the possibility of being affected by ransomware, I get a bad feeling.	FEAR4
I fear being affected by ransomware.	FEAR5
Defense Avoidance [8]	
I do not want to think about my risk of being affected by ransomware.	DA1
I doubt if ransomware is a danger to me.	DA2
I do not want to protect myself from ransomware actively.	DA3
I do not want to think about the consequences of ransomware.	DA4
Behavioral Intention [11]	
In order to protect myself against ransomware, I intend to use antivirus programs for the next 3 months actively.	BI1
In order to protect myself against ransomware, I will probably use antivirus programs in the next 3 months actively.	BI2
In order to protect myself against ransomware, I plan to use antivirus programs in the next 3 months actively.	BI3
In order to protect myself against ransomware, I plan to actively create backups in the next 3 months.	BI4
In order to protect myself against ransomware, I plan to create backups within the next 3 months actively.	BI5
To protect myself against ransomware, I plan to create backups in the next 3 months actively.	BI6