Mitigating the ransomware threat: a protection motivation theory approach

Jacques Ophoff
Mcguigan Lakay

This is the Author Accepted Manuscript of a conference paper published in Information security: 17th International conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, revised selected papers

The final authenticated version is available online at https://doi.org/10.1007/978-3-030-11407-7_12

Mitigating the Ransomware Threat: A Protection Motivation Theory Approach

Jacques Ophoff[1][0000-0003-0634-5248] and Mcguigan Lakay[2]

University of Cape Town, Cape Town, South Africa
[1]jacques.ophoff@uct.ac.za, [2]mcguigan.lakay@uct.ac.za

Abstract. Ransomware has emerged as one of the biggest security threats to organizations and individuals alike. As technical solutions are developed the creators of ransomware are also improving the sophistication of such attacks. A combination of technical and behavioral measures is required to deal with this problem. This study investigates computer users' motivation to adopt security measures against ransomware, using protection motivation theory (PMT) as a theoretical foundation. We conducted empirical research, using a survey methodology, collecting data from 118 respondents. Using partial least squares structural equation modelling our analysis provides support for several factors influencing protection motivation in this context. These include perceived threat severity and perceived threat vulnerability, mediated by fear. Self-efficacy is shown as a significant coping factor. Maladaptive rewards and response costs both have a significant negative influence on protection motivation. The results provide support for the use of fear appeals and PMT to influence protection motivation in the context of ransomware threats.

Keywords: Ransomware, Malware, Cybersecurity, Protection Motivation Theory, Fear Appeal.

1 Introduction

Data is one of the most valuable assets in any organization. Ensuring the availability of data is a main objective of information security [1]. There are numerous threats to the availability of data, but one of the fastest growing in recent years is ransomware. Ransomware is a type of malware which makes data inaccessible until the victim pays a ransom to the attacker [2].

Ransomware has impacted organizations worldwide and across industries. Since 2014 there has been significant growth in the number of reported attacks [2]. There have been several high-profile attacks, including major incidents in the healthcare industry [3]. Attacks have also targeted users and their personal data, increasingly through mobile devices [4, 5]. Considering the bring your own device (BYOD) trend this presents another attack vector for organizations to manage. While detection and recovery tools have improved, there are indications that ransomware attacks are becoming more sophisticated and will continue to be a threat to organizations and individuals [5, 6].

Mitigating ransomware is as much a behavioral as a technical problem. From a behavioral information security perspective the focus is on users and their performance of important security measures [7, 8]. Several measures are advised in response to the increasing number of ransomware attacks, such as backing up critical data and not opening suspicious (phishing) email links or files. However, there is evidence that technically unsophisticated users do not implement such measures [4].

In this paper we investigate computer users' motivation to adopt security measures against ransomware from a behavioral information security perspective. We use the term computer user broadly to include both employees using organizational systems as well as individual users of personal devices. We address the following research question: *Which factors influence user motivation to adopt security measures against ransomware attacks?* To answer this question, both theoretically and empirically, we base our research on protection motivation theory (PMT). We use PMT because of its ability to explain voluntary security-related actions, for instance the adoption of anti-spyware [9] and backing up data [10].

The remainder of this paper is organized as follows. First, the conceptual and theoretical background will be presented. This includes our research hypotheses and conceptual model. Next, we discuss the research methodology that was used. This is followed by data analysis and a discussion of the results. Lastly, the conclusion summarizes the research contributions.

2 Background

In the following subsections we first provide some context around ransomware and end-users' behavioral security issues. Then we discuss PMT as theoretical foundation for the study. This is followed by the hypotheses for the study.

2.1 Ransomware

Ransomware is a type of malware that threatens the availability of data, with the intention of gaining a financial reward. To gain access to a system social engineering tactics are frequently used to exploit a potential victim [11]. Once ransomware is installed on a system it encrypts data files and demands payment in return for a decryption key [5]. The typical method of ransom payment is in a digital currency, such as Bitcoin, as it provides anonymity and can be used globally [12]. This also means that there is no guarantee of receiving a valid decryption key even if the ransom payment is made.

Ransomware can have a severe impact on organizations, potentially halting all operations. This often damages the organizations reputation, leading to further financial losses [5]. Small and under resourced organizations are prone to being targeted, especially if it is known that they are willing to pay the ransom [13]. Although there are technical measures to mitigate ransomware, such as anti-malware software, these are often temporary as ransomware is continuously evolving [4]. Due to the lack of a

permanent technical solution to ransomware, only awareness and protective behaviors of users can help to reduce the impact of ransomware attacks [8].

The central idea behind ransomware is to leverage the victim's fear of data loss. The current problem is that users do not necessarily put in effort and time to secure their information assets [14]. Conceivably users are not aware of how vulnerable they are or how severe ransomware can be. From a protection motivation perspective, manipulating individuals' fear has been shown to lead to change in behavioral intentions [9]. In this regard the intention is to get users to adopt security measures when interacting with their information assets, to avoid falling victim to ransomware attacks. This notion of using fear to modify security behavior is one of the main research areas in behavioral information security and forms the foundation of PMT.

2.2 Protection Motivation Theory

PMT was developed by Rogers [15] with the objective of promoting healthy behaviors. It is applicable to any threat-related study for which there is a practical recommended action that can be carried out. The theory conceptualized that persuasive communication, using a fear appeal, initiates a cognitive appraisal process involving the threat and a coping response [15].

The threat-appraisal process is triggered by a fear appeal message which may, or may not, induce fear. Threat-appraisal consists of the perceived threat vulnerability and perceived threat severity constructs [10, 15]. PMT suggests that fear could be predicted as it is an emotion in response to a threat. Fear as a stimulus can influence an individual's intention to take recommended protective actions.

The coping-appraisal evaluates the belief that a recommended response can prevent the threat [15]. Coping-appraisal consists of the response efficacy, self-efficacy, and response costs constructs [10]. A user will engage in protection motivation if response efficacy and self-efficacy outweigh the response costs.

In behavioral information security research PMT has been used and extended [e.g. 16] to motivate employees and individuals to adopt security measures. Boss et al. [10] identifies two versions of PMT: the core model in its fundamental form and the full model (nomology). The core model consists of perceived threat severity, perceived threat vulnerability, response efficacy, self-efficacy, response costs, and protection motivation. This model is partially supported by a number of information security studies [e.g. 17, 18], but contains little or no emphasis on fear appeal manipulations. The full model includes fear, as a partial mediator between perceived threat severity, perceived threat vulnerability and protection motivation, as well as maladaptive rewards. The full model was used in this study.

2.3 Hypotheses Development and Conceptual Model

The threat of ransomware is used in combination with PMT in this study. Protection motivation includes the intention to adopt security measures aimed at mitigating data loss caused by ransomware. Measures could include backing up data, changing default passwords, updating the operating system and software applications, using an

anti-virus tool to scan the device for malware, setting user access controls, using a firewall, and using popup blockers in web browsers [14]. This study will consider two of these measures: using anti-malware software and backing up data.

Threat-appraisal. In the full PMT model the threat-appraisal process consists of perceived threat severity, perceived threat vulnerability, and maladaptive rewards. Perceived threat severity refers to the degree of the consequences if the threat causes harm [19]. In the ransomware context the loss of data can lead to severe organizational consequences, such as halting of business operations and reputational damage. Perceived threat vulnerability refers to users' judgment of the probability of being exposed to the threat [19]. In our research context this refers to users' assessment of the probability of their devices being exposed to ransomware. We hypothesize that:

H1a: An increase in perceived severity of ransomware threats increases protection motivation.
H1b: An increase in perceived vulnerability to ransomware threats increases protection motivation.

Fear is a negative emotion that can be triggered if the perceived threat is relative to the individual [20]. A ransomware fear appeal is a stimulus designed to trigger the threat-appraisal and coping-appraisal processes [19]. This could be achieved by informing users of the consequences of ransomware and appropriate security measures. Fear influences both protection motivation and acts as a mediator between the threat and protection motivation [10]. With respect to fear we hypothesize that:

H2a: An increase in perceived severity of ransomware threats increases perceived fear.
H2b: An increase in perceived vulnerability to ransomware threats increases perceived fear.
H3: An increase in fear increases protection motivation.

Maladaptive rewards can influence the threat appraisal process depending on the user's assessment of the reward if the recommended action is ignored. The user may opt for the maladaptive reward if it holds more weight than the perceived threat [10]. An example is when a user chooses to install software from an unknown source, even though it may contain hidden ransomware. Therefore, we hypothesize:

H4: An increase in maladaptive rewards decreases protection motivation.

Coping-appraisal. The coping-appraisal process consist of the response efficacy, self-efficacy, and response costs. Response efficacy is the confidence users have in the effectiveness of the recommendation provided in the fear appeal. Self-efficacy is the confidence or belief of users that they can perform the recommendation. Response costs are the expenses users experience to implement the recommendation, such as time and effort [10]. Belief in the effectiveness of security recommendations and the user's ability to perform them is required for a positive appraisal [19]. In the context

of preventative measures against ransomware, if users believe that making regular backups of their data and using anti-malware software will be useful to minimize the severity of ransomware, there will be a greater chance of protection motivation. We hypothesize that:

H5a: An increase in response efficacy increases protection motivation.
H5b: An increase in self-efficacy increases protection motivation.
H5c: An increase in response costs decreases protection motivation.

Based on the above discussion, Fig. 1 presents our conceptual research model. Based on the constructs from PMT the model predicts several factors which influence users' protection motivation in the context of ransomware.

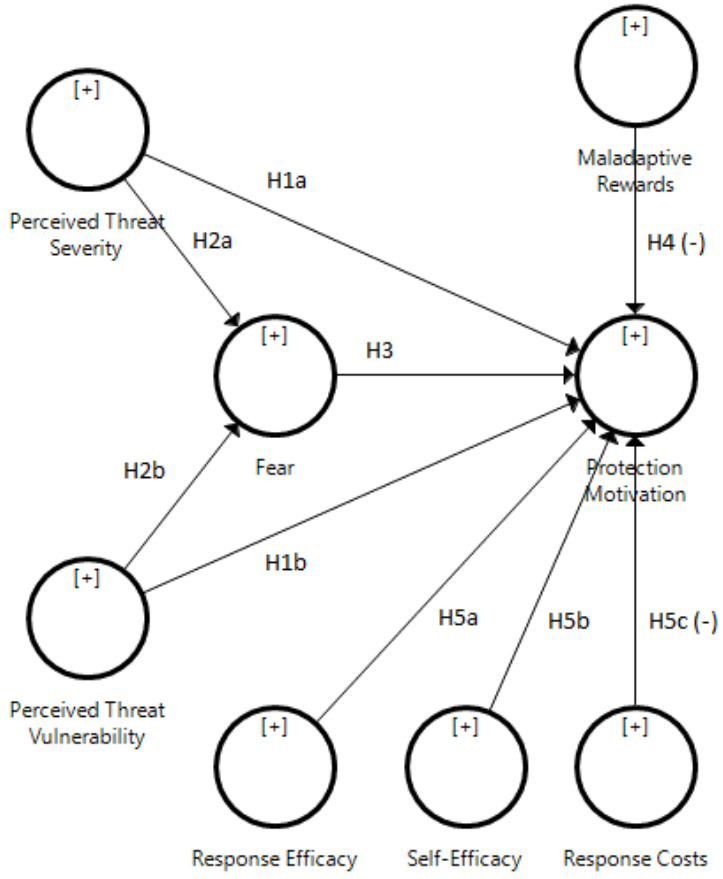

Fig. 1. Conceptual model (based on Boss et al. [10]).

3 Methodology

We evaluated our conceptual model empirically, using a cross-sectional survey. Data was collected from a random sample of staff and students at a large research university. The university was deemed an appropriate organization as it had faced regular ransomware attacks, targeting both staff and students.

We developed a fear appeal for the survey, which is shown in Fig. 2. The fear appeal is a combination of ransomware communications (previously sent by the university) and a typical ransom message (usually seen after a successful attack has encrypted data). Information about the threat was conveyed by both parts, while recommended actions were contained in the (university) communication.

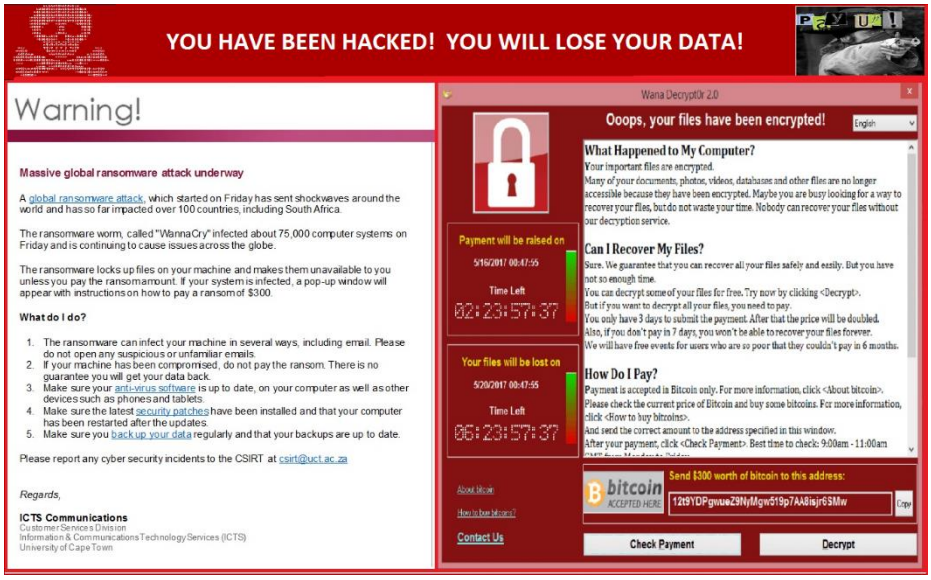

Fig. 2. Fear appeal with recommended actions.

Respondents were asked to study the fear appeal before proceeding with the survey. The fear appeal was followed by questions related to each of the model constructs. To ensure research validity and reliability the item wording was based on Boss et al. [10]. The constructs and related measurement items are shown in Table 1. Each item was measured using a 7-point Likert scale. The survey concluded with several demographic and device usage questions.

Table 1. Study measurement items.

Construct	Code	Items (R = reverse coded)
Perceived threat severity (PTS)	PTS1	If I were to lose data from my hard drive, I would suffer a lot of pain.
	PTS2	Losing data would be unlikely to cause me major problems. (R)
	PTS3	If my computer were infected by ransomware, it would be severe.
Perceived	PTV1	I am unlikely to lose data in the future. (R)

threat vulnerability (PTV)	PTV2	My chances of losing data in the future are less likely. (R)
	PTV3	It is likely that my computer will become infected with ransomware.
Maladaptive rewards (MR)	MR1	Not using an anti-malware application saves me time.
	MR2	Not using an anti-malware application saves me money.
	MR3	Not using an anti-malware application keeps me from being confused.
Fear (F)	F1	I am afraid of ransomware.
	F2	My computer might be seriously infected with ransomware.
	F3	My computer might become unusable due to ransomware.
	F4	I am frightened about the prospect of losing data from my computing device.
	F5	I am worried about the prospect of losing data from my computing device.
Response efficacy (RE)	RE1	Backing up my hard drive is a good way to reduce the risk of losing data.
	RE2	If I were to back up my data at least once a week, I would lessen my chances of data loss.
	RE3	When using anti-malware software, a computers data is more likely to be protected.
Self-efficacy (SE)	SE1	Anti-malware software is easy to use.
	SE2	Anti-malware software is convenient to use.
	SE3	I am able to use anti-malware software without much effort.
Response costs (RC)	RC1	The benefits of backing up my hard drive at least once a week outweigh the costs. (R)
	RC2	I would be discouraged from backing up my data during the next week because it would take too much time.
	RC3	Taking the time to back up my data during the next week would cause me too many problems.
Protection motivation (PM)	PM1	I intend to back up my hard drive during the next week.
	PM2	I do not wish to back up my data during the next week. (R)
	PM3	I intend to use anti-malware software in the next three months.
	PM4	I predict I will use anti-malware software in the next three months
	PM5	I plan to use anti-malware software in the next three months.

The survey was implemented online using the Qualtrics platform.[1] A pilot study was conducted to pretest the survey fear appeal, item wording, and flow. After minor modifications a survey link was distributed via email.

4 Data Analysis and Results

A total of 234 responses were collected. From these 94 incomplete responses were removed. A further 22 responses were removed due to not answering a control question correctly, leaving a final dataset of 118 responses for analysis. There were many responses in which no questions were answered, which could be due to a reluctance to read the fear appeal and no incentives being offered.

[1] https://www.qualtrics.com/

The demographic data indicates a younger (59 percent aged below 25) and slightly more female (52 percent) sample. Most of the respondents were regular users of computing devices. A summary of the demographic data is provided in Table 2.

Table 2. Demographic data

Demographic	Items	Count	Percentage
Gender	Male	55	47%
	Female	62	52%
	Prefer not to answer	1	1%
Age	Under 18 years	0	-
	18-24 years old	70	59%
	25-34 years old	27	23%
	35-44 years old	13	11%
	45-54 years old	6	5%
	55-64 years old	2	2%
	65 years or older	0	-
Primary role	I am an undergrad student	65	55%
	I am a post-grad student	33	28%
	I am an academic staff member	2	2%
	I am an admin staff member (Non-IT)	7	6%
	I am an IT staff member	11	9%
Primary device	Smartphone / Mobile phone	22	19%
	Tablet	2	2%
	Personal Computer	16	14%
	Laptop	78	66%
Device experience	Less than 1 year	5	4%
	1-2 years	11	9%
	3-5 years	12	10%
	6-10 years	28	24%
	More than 10 years	62	53%
Device use	Less than 1 hour a day	0	-
	1-2 hours a day	6	5%
	3-5 hours a day	35	30%
	More than 5 hours a day	77	65%

Data analysis was performed using partial least squares structural equation modelling (PLS-SEM). PLS-SEM focuses on explaining the variance in dependent variables [21]. The approach is suitable for validating predictive models and can be used with small sample sizes [22]. The tool used for analysis was SmartPLS [23]. In analyzing our data we followed the recommended multi-stage process [22], which starts with estimating the path model and assessing the reflective measurement model.

4.1 Analysis of the Measurement Model

A model is said to be reflective if the indicators are highly correlated and interchangeable [21]. Due to the high correlations their reliability and validity should be thoroughly examined. The first criterion to be evaluated is internal consistency relia-

bility (CR). In this regard we examined composite reliability, with all constructs above the recommended threshold (0.70). Next we examined convergent validity, during which three indicators with weak outer loadings (F2 and F3 <0.40; RE2 <0.70) were removed. The remaining indicators' loadings were acceptable. The average variance extracted (AVE) for all constructs were above the recommended threshold (0.50). Finally, discriminant validity was assessed using the Fornell-Larcker criterion. This showed that all constructs were within acceptable ranges. The above results are summarized in Table 3. All model evaluation criteria were met, providing support for the measures' reliability and validity.

Table 3. Reliability and validity assessment results.

			Fornell-Larcker Correlations							
Cons.	**CR**	**AVE**	**F**	**MR**	**PTS**	**PTV**	**PM**	**RC**	**RE**	**SE**
F	0.896	0.742	0.861							
MR	0.818	0.601	-0.065	0.775						
PTS	0.808	0.585	0.666	-0.139	0.765					
PTV	0.85	0.658	0.338	0.087	0.218	0.811				
PM	0.89	0.627	0.29	-0.599	0.234	-0.036	0.792			
RC	0.849	0.652	-0.096	0.235	-0.045	-0.014	-0.482	0.808		
RE	0.759	0.615	0.201	-0.28	0.198	-0.144	0.415	-0.152	0.784	
SE	0.877	0.705	0.103	-0.581	0.052	-0.226	0.582	-0.293	0.418	0.839

4.2 Analysis of the Structural Model

The structural model was tested to estimate the path coefficients, which calculates the strength of the relationships between constructs. The coefficients of determination (R^2) values indicate that the model explains approximately 48 percent of the variance for fear, and 59 percent for protection motivation. Compared to previous information security studies using PMT, the values show a medium to high effect size [10]. In addition, the f^2 effect size showed a medium effect of maladaptive rewards (0.195) and response costs (0.196) on protection motivation, as well as a large effect of perceived threat severity on fear (0.711).

Bootstrapping with 5,000 samples [21] was used to test the significance of the structural paths (hypotheses). The results indicate that only H1a, H1b, and H5a are not significant. The PLS path modelling estimation, including path coefficients and p-values, is shown in Fig. 3. The results of hypothesis testing are summarized in Table 4.

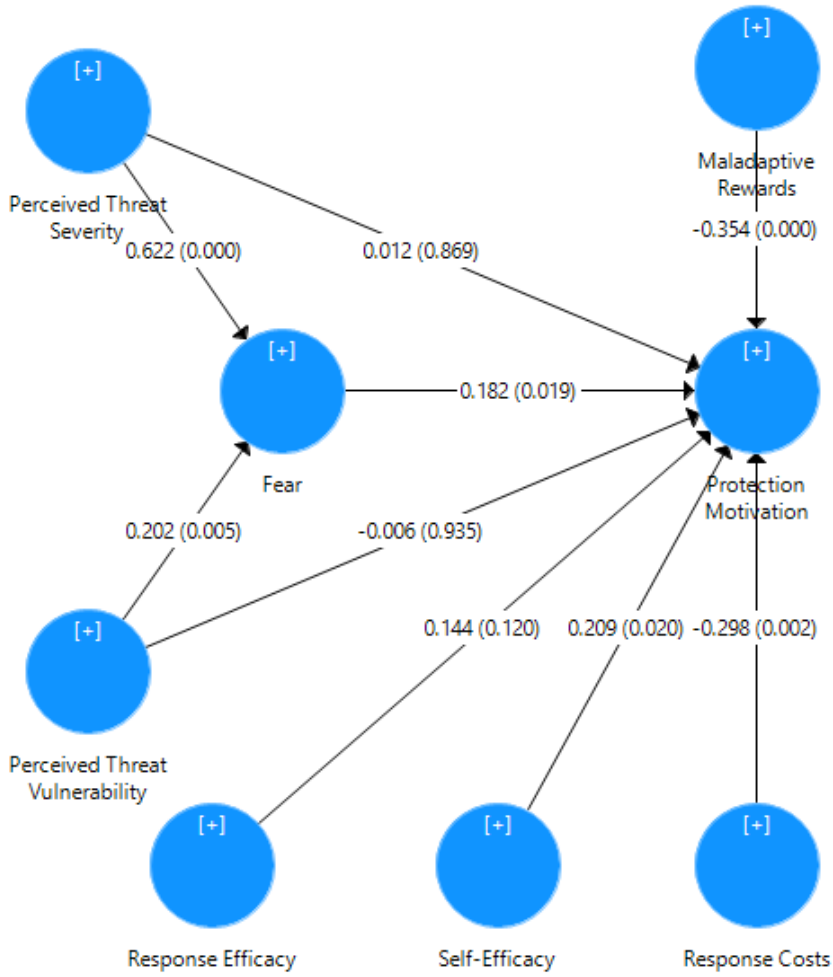

Fig. 3. Structural model analysis.

Table 4. Overview of findings.

Hypothesis	**Path Coefficient**	**T Value**	**P Value**	**Supported?**
H1a: PTS => PM	0.012	0.165	p > 0.1	Not supported
H1b: PTV => PM	-0.006	0.082	p > 0.1	Not supported
H2a: PTS => F	0.622	9.663	p < 0.001***	Supported
H2b: PTV => F	0.202	2.813	p < 0.01**	Supported
H3: F => PM	0.182	2.353	p < 0.05*	Supported
H4: MR => PM	-0.354	3.535	p < 0.001***	Supported
H5a: RE => PM	0.144	1.557	p > 0.1	Not supported
H5b: SE => PM	0.209	2.33	p < 0.05*	Supported
H5c: RC => PM	-0.298	3.089	p < 0.01**	Supported

4.3 Discussion

The results show strong support for the application of PMT in the context of a ransomware threat. The perceived threat severity and vulnerability seems to have no direct influence on protection motivation, but does strongly influence fear as an emotional response. From our results there is evidence that fear acts as a mediator between the threat and protection motivation [10]. H2a and H2b explain that a user's perception of fear of a threat must be high to motivate the user to perform a recommended behavior as provided in the fear appeal message. The findings demonstrate that that fear is an independent and dependent multi-dimensional construct [7] which is affected significantly by perceived threat severity and perceived threat vulnerability.

It is interesting to note the significant influence of maladaptive rewards and response costs on protection motivation. This indicates that there are significant barriers to overcome to influence users. We investigated this further using multigroup analysis [21], looking at the influence of the users primary device. When comparing smartphones and laptops there is a significant difference ($p < 0.05$) in the effect of maladaptive rewards (for smartphones) and perceived threat severity, where the perception of a threat is less on smartphones.

In terms of coping-appraisal response efficacy was not significant, which could indicate that respondents did not fully understand the recommendations. Due to the coping responses being backing up data and using anti-malware software, a user's perception could be negatively impacted as there have been recent reports on ransomware attacks [5].

A fear appeal with recommended behaviors to protect oneself from ransomware was introduced to influence users towards protection motivation. The fear appeal may have induced fear which trigged the processes in PMT. However, the fear appeal message could have been ignored by the user. Respondents' answers would then be based on their personal experiences with similar threats and their means of dealing with those threats.

Protection motivation is a dependent variable which is significantly affected by fear as well as some of the other constructs, as seen in the analysis section. In this study perceived threat severity, perceived threat vulnerability, and response efficacy did not play a significant role in influencing protection motivation.

5 Conclusion

This study examined the threat of ransomware, analyzing the factors that could influence protection motivation in users. This is motivated by the fact that the mitigation of ransomware requires both technical solutions as well as behavioral changes. The study used PMT as a theoretical basis. Based on our empirical results it was shown that PMT is a good foundation in this context.

Several factors were shown to significantly influence user motivation to adopt security measures against ransomware attacks. These include perceived threat severity and perceived threat vulnerability, mediated by fear, as part of the threat-appraisal

process. Self-efficacy was shown as a significant factor in the coping-appraisal process. Maladaptive rewards and response costs both had a significant negative influence on protection motivation.

This study has several limitations which present promising directions for future research. It could be argued that the research sample was limited and too homogenous, consisting only of university staff and students. However, within university environments ransomware threats have been a problem and thus it is argued as a valid organizational context. Future research could expand the study using a larger and more heterogenous sample.

We created a custom fear appeal, but did not extensively test differences in the design of this message. Future research could examine this aspect of PMT in more detail, potentially using an experiment to test differences in fear appeal designs. A theoretical basis for the design which ties in with PMT would add credibility and extend existing behavioral information security research.

In literature numerous recommended actions are given to mitigate ransomware. We only focused on two such recommendation, the use of anti-malware software and backing up data. Future studies could expand this with questions related to phishing emails, installing operating system and software updates, etc. In this way protection motivation can be formalized as a formative construct.

6 Acknowledgement

This work is based on the research supported wholly / in part by the National Research Foundation of South Africa (Grant Numbers 114838).

References

1. Whitman, M.E., Mattord, H.J.: Principles of Information Security. Cengage Learning, Boston, MA (2011).
2. Al-rimy, B.A.S., Maarof, M.A., Shaid, S.Z.M.: Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security. 74, 144–166 (2018).
3. Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO), https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.
4. Kharraz, A., Robertson, W., Kirda, E.: Protecting against Ransomware: A New Line of Research or Restating Classic Ideas? IEEE Security Privacy. 16, 103–107 (2018).
5. Mansfield-Devine, S.: Ransomware: taking businesses hostage. Network Security. 2016, 8–17 (2016).
6. Nadeau, M.: 11 ransomware trends for 2018, https://www.csoonline.com/article/3267544/ransomware/11-ways-ransomware-is-evolving.html.
7. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security. 32, 90–101 (2013).

8. Fimin, M.: Are employees part of the ransomware problem? Computer Fraud & Security. 2017, 15–17 (2017).
9. Johnston, A.C., Warkentin, M.: Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly. 34, 549-A4 (2010).
10. Boss, S.R., Galletta, D.F., Benjamin Lowry, P., Moody, G.D., Polak, P.: What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors. MIS Quarterly. 39, 837–864 (2015).
11. Gallegos-Segovia, P.L., Bravo-Torres, J.F., Larios-Rosillo, V.M., Vintimilla-Tapia, P.E., Yuquilima-Albarado, I.F., Jara-Saltos, J.D.: Social engineering as an attack vector for ransomware. In: 2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON). pp. 1–6 (2017).
12. Brewer, R.: Ransomware attacks: detection, prevention and cure. Network Security. 2016, 5–9 (2016).
13. Simmonds, M.: How businesses can navigate the growing tide of ransomware attacks. Computer Fraud & Security. 2017, 9–12 (2017).
14. Crossler, R.E., Bélanger, F., Ormond, D.: The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. Information Systems Frontiers. 1–15 (2017).
15. Rogers, R.W.: A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology. 91, 93–114 (1975).
16. Aurigemma, S., Mattson, T.: Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. Computers & Security. 73, 219–234 (2018).
17. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems. 18, 106–125 (2009).
18. Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management. 49, 190–198 (2012).
19. Rogers, R.W.: Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. Social Psychophysiology. 153–176 (1983).
20. Witte, K.: Fear control and danger control: A test of the extended parallel process model (EPPM). Communication Monographs. 61, 113–134 (1994).
21. Hair Jr, J.F., Hult, G.T.M., Ringle, C.M., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling. SAGE Publications, Inc, Los Angeles (2016).
22. Hair Jr, J.F., Sarstedt, M., Hopkins, L., Kuppelwieser, V.G.: Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European Business Review. 26, 106–121 (2014).
23. Ringle, C.M., Wende, S., Becker, J.-M.: SmartPLS 3. SmartPLS GmbH (2015).