Preprint: Zarifis A. & Cheng X. (2018) 'The impact of extended global ransomware attacks on trust: How the attacker's competence and institutional trust influence the decision to pay', Proceedings of the Americas Conference on Information Systems (AMCIS)

The Impact of Extended Global Ransomware Attacks on Trust: How the Attacker's Competence and Institutional Trust Influence the Decision to Pay

Completed Research

Alex Zarifis
University of Mannheim, Germany
azarifis@mail.uni-mannheim.de

Xusen Cheng
University of International Business and Economics, China
xusen.cheng@uibe.edu.cn

Abstract

The standardization, interconnectivity and pervasiveness of information systems, combined with the increasing ability to collect and utilize data, enhance the value they offer a user. These strengths however can also be turned into a weakness and vulnerability by ransomware (RW). RW can utilize the functionality of current systems both to infect them but also to increase the magnitude of the attack. This research proposes a model of the impact of the RW attack on the user's trust, which in turn has an effect on their decision to pay the ransom or follow the guidance from the relevant institutions. The model shows that the effectiveness of the attack, the trust in the competence of the attacker and ransomware demands that are reasonable and easy to fulfil, positively influence the intention to pay the ransom. The initial institutional response, institutional trust and institutional solution influence the intention to follow the institutional guidance.

Keywords

Ransomware, malware, e-commerce, trust, WannaCry, Petya.

Introduction

On the fifth of May 2017 extensive ransomware (RW) attacks impacted many countries. Targets included public and private organizations around the world including hospitals, carmakers and train operators across Europe. Millions of users, customers and patients were impacted directly by the prolonged attack that harmed the victims in many ways. Most people around the world however had not visited a hospital, would not notice that their car took a few days longer to make, or bought a train ticket. Almost everyone however had turned on their computers and TVs and seen the RW message requesting a payment on their screen from news outlets and social media. It was not just these hundreds of organizations that were held ransom but also trust in the public and private institutions such as regulators, that had until then provided people with reliable digital services. If reputable organizations that have a strong bond with millions, like a carmaker and a train operator, can be compromised what else is vulnerable? Are the regulations, operating systems, online platforms and the internet infrastructure itself safe?

RW is a growing problem with incidents increasing yearly since 2012. Some reports claim approximately two in five organizations have been targeted by RW attacks (Simmonds 2017). The breadth of use and reliance on technology, and the inevitability of bugs in the software that create vulnerabilities, mean it is difficult to be confident of avoiding such attacks (Orman 2016). The attack in May 2017 using WannaCry RW was considered technologically basic but this was soon followed by the more sophisticated Petya GoldenEye. There are many types of RW that can infect servers, specific PCs and mobile devices. Most of these ransoms require payment by Bitcoin. This digital currency and payment method, like RW, is not fully

controlled or regulated by institutions. This may further compound the erosion of trust in the control and influence of institutions.

RW raises many technical issues on an organization's software and hardware, as well as the national infrastructure. There is also an impact on an individual's trust. Trust has been found to be an important prerequisite to transactions, particularly online (Pavlou 2003). RW has been explored primarily in the area of security, both in relation to the relevant information systems and the role of members of the organization in strengthening or weakening security (Mustaca 2014). The influence on the individuals outside of the infected organizations such as consumers, users, patients or other stakeholders has not been sufficiently explored. As the scale and severity of these attack grows the influence on the individual, particularly their trust becomes more important. The importance of trust emerges from uncertainty and its significance is elevated when the degree of uncertainty increases (Jarvenpaa et al. 1999). A RW attack increases uncertainty for many users, especially those directly affected. Given the national or global nature of these attacks trust in institutions is affected, not just trust in individual organizations. This research explores and evaluates the impact of extended global RW attacks, such as the case of the May 2017 attacks, on institutional trust and the intention to pay the ransom. The proposed model shows how the effectiveness of the attack, the trust in the competence of the attacker and the value of the RW solution influence the user's intention to pay the ransom. On the other hand, the initial response of the institutions, institutional trust and the value of the solution offered, influences the user's decision to follow the institutional solution.

Theoretical Background

The volume of data generated and utilized is expanding. So are the devices that generate and utilize these data. The benefits we receive and our dependence on these data increases in line with this expansion. This applies to both professional and personal lives as highlighted when hospitals are targeted. Therefore, while malicious attacks are not new, the impact on an individual's trust is significant. The individual may already feel vulnerable due to other threats like privacy issues (Khokhar et al. 2016). From the perpetrator's perspective, the scalability of the attacks means that more widely used systems, such as Google Android or Microsoft Windows 10, are more appealing targets (Mercaldo et al. 2016). This suggests large scale attacks, targeting large organizations globally, may continue to happen.

Ransomware attack

RW is a form of malware software that is designed to covertly collect data and financially extort the victim (Mercaldo et al. 2016). The attack can be initiated in a number of ways such as phishing emails, malicious downloaded programs, malicious embedded adverts that execute JavaScript, 'watering-hole attack' and 'web-drive by' (Erridge 2016). The global RW attacks of WannaCry and Petya GoldenEye spread quickly by utilizing an exploit in an operating system, that allowed quick filesharing from one computer to another and bypassed the security of the new victim. This meant computers with no security vulnerabilities introduced by the user, updated security and antivirus, could be infected. The technology that makes this crime possible includes the cryptography that makes the victims data inaccessible. It may block access to data or all the system's functionalities until a ransom is paid. Some sophisticated RW attacks target the most critical systems and data. Furthermore, data can be stolen including pictures and actions can be taken such as taking photos with the device's camera. The specific technologies used are evolving with more sophisticated and elaborate attacks emerging. The attack in May 2017 using WannaCry RW was basic but this was followed by the more sophisticated Petya GoldenEye. While Wannacry encrypted some data and had a kill switch, Goldenye encrypted the whole disc, deleted the event logs and did not have a universal kill switch. The damage caused is significant with one fifth of victims completely stopping their operations for a period (Simmonds 2017). Other intentions may be concealed under an apparently typical RW such as stealing data, installing spyware or installing dormant malware for use in future attacks.

Ransomware response

A global RW attack such as the one the May 2017 can be described as a disaster with far reaching consequences. A solution may take weeks and may not be comprehensive. Therefore, the initial response from the institutions is both distinct from the solution and important. Furthermore, in many disasters the response can have an influence on the victim comparable to the disaster itself. The victim is under pressure (Wecksten et al. 2016) and may respond extremely positively to helpful support and extremely negatively

to what is perceived as unhelpful. The institutions are part of an 'ecosystem' that supports secure e-commerce. They support an organization's information systems such as the operating system, the enterprise system, the antivirus software, the local network and the international network. The public and private institutions that are responsible for oversight and support the normal situation, are also part of this 'ecosystem'. The success of maintaining situational normality, depends on this collaboration being coordinated. Effective collaboration is often critical in disaster management (Simon et al. 2009). The solution emerges from a forensic investigation of the attack (Orman 2016). The victim must inform the relevant institutions and not keep the attack secret and pay the ransom. Therefore, there is a necessary collaboration between the victim and the institutions in developing and implementing the solution. As trust is important in most forms of collaboration, it is central to responding to the attacks successfully.

The effect of extended, global ransomware attacks on institutional trust

While the attack uses a software virus to hold an organization's software 'hostage', this is not just about information systems. The people involved are an equally important part of the puzzle, as the attacker's success ultimately depends on intimidation (Simmonds 2017). The perception of the threat can be more significant than the factual threat. Here, we focus on the victim's perspective not the system perspective.

In the area of e-commerce one useful explanation of trust is that it is the willingness to depend, based on a belief in the reliability and benevolence (Pavlou and Gefen 2004). One important point this definition makes, is that trust depends both on the perceived intention but also the ability to deliver what is agreed on. Initial research into trust centered on technology adoption (McKnight et al. 2002) while more recent research also evaluated trust in post adoption scenarios (Thatcher et al. 2011). For the case of the influence of RW attacks, the models on postadoption are more suitable, as this attack impacts existing users and consumers that have already trusted the institutions.

Institutional trust is formed by situational normality and structural assurance (McKnight et al. 2002). These two components of institutional trust are dependent on the context of the relationship. For example, they are different when evaluating health intermediaries (Song and Zahedi 2007) or making a purchase with a digital currency like Bitcoin (Zarifis et al. 2014). Situational normality is formed by competence, benevolence, integrity and the more general situation. Structural assurance is the belief of the user or consumer, that the environment they are using, with various information systems, is safe. This covers processes, procedures, contracts, guarantees, promises and legal recourse (McKnight et al. 2002).

Consumer trust was earned by organizations and the institutions that support them through the quality of the service and the level of security and privacy provided. Global RW attacks however, offer a challenge to this. This challenge may not be fully explained by the existing trust models that were primarily focused technology adoption or attitude towards technology. In some of these attacks, reputation harm may be the main motive and not financial gain (Erridge 2016). It is possible that in such attacks the ransom is there to conceal the real purpose.

Research Model

Trust has been defined as a belief in the competence, benevolence and integrity of an organization or an individual (Mayer et al. 1995). While the attacker would not be expected to create a belief in their benevolence and integrity with their action, the effectiveness of the attack may create a belief in their competence. The competence in information systems to implement the attack would indicate a competence in discontinuing the attack. Therefore, the first hypothesis is:

H1: The effectiveness of the attack will increase the victim's trust in the competence of the attacker.

For the attacker to succeed in encrypting the victim's files they need to overcome the security many institutions have in place. These institutions include the antivirus supplier, the operating systems provider, organizations related to the internet and other organization, public or private which may have identified vulnerabilities and then unintentionally revealed them. By succeeding in the attack, the trust in these institutions is reduced. Therefore, the second hypothesis states:

H2: The trust in the competence of the attacker will decrease the victim's trust in the institutions.

The victim will need to trust the competence of the attacker so that they pay the ransom. The victim will need to believe that the attacker is in control and can discontinue the attack when the payment is made.

The victim must also believe the decryption keys will be given and that the encryption can be reversed. If the victim concludes that there is nobody in control of this attack and it is an uncontrolled, self-propagating, virus they may not want to transact. Therefore, the third hypothesis states:

H3: The trust in the competence of the attacker will increase the victim's intention to pay the ransom.

The RW attack is experienced by the victim while the solution offered to them, if they pay the ransom, has not been experienced before the decision to pay or not is made. The belief of the victim in relation to the attack is based on an experience, while the belief of the solution offered by the attacker is based on their expectation of an outcome. Therefore, while the RW attack and the offer to discontinue the attack both come from the attacker they are two separate constructs. Therefore, the fourth hypothesis states:

H4: The perceived effectiveness of paying the ransom will have a negative effect on the perceived effectiveness of the institutional solution.

The nature of the ransom itself influences the decision to pay it. The amount, the currency and payment method are considered when making a decision. The payment process of the ransom can include elements of technology adoption due to its nature. A high amount and payment in a currency that is relatively difficult to acquire and make a payment like Bitcoin, may have a negative influence on the decision to pay. There has been anecdotal evidence of organizations struggling to find a sufficient number of Bitcoins to make a ransom payment. Therefore, the fifth hypothesis states:

H5: The perceived effectiveness of paying the ransom will have a positive influence on paying the ransom.

The way the victim's trust in the institutions is influenced by the RW attack can be a mirror image of the victim's trust in the attacker. As illustrated in figure one, certain actions shape trust and ultimately influence the decision to pay the ransom or follow the institutions guidance. The initial response of the institutions after the RW attack will influence the trust of the victim in the institutions. A positive response would include elements of disaster management. This response can be organized, coordinated and reassuring, increasing trust (Aliakbarlou et al. 2017). It can be useful to the victim even if it stops short of providing a comprehensive solution. A positive response can offer clear information; this information can come from the institutions first, before it is released by another source like a blogger and there can be no information withheld. Alternatively, it can be chaotic. For example, one institution may blame the software provider for not offering the necessary support and the software provider may blame the organization for using outdates systems. Therefore, the sixth hypothesis states:

H6: The perceived effectiveness of the initial institutional response to the RW attack will increase the victims trust in the institutions.

A higher level of institutional trust will make the victim follow the guidance offered because a positive outcome will appear more likely. The trust in the institution relevant here covers competence, benevolence and integrity. This is unlike the trust in the attacker which is limited to trust in their competence. Institution based trust is formed by situational normality and structural assurance. Situational normality suggests a positive outcome because of an ordered, normal and positive Internet environment (McKnight et al. 2002). Structural assurance refers to safeguards such as guarantees, regulations and legal remedy intended to support a positive outcome. It has been validated that institutional trust strengthens trusting beliefs which in turn reinforce trust related behaviors (McKnight et al. 2002). As the attacker and institutions have opposing objectives, an increase in the trust in the former reduces trust in the latter:

H7: The institutional trust will increase the victim's intention to follow institutional guidance.

H8: The institutional trust will decrease the victim's trust in the competence of the attacker.

The victim will evaluate the effectiveness of the solution offered by the institutions. A solution that emerged from outside the institutions, like a security expert, but was endorsed by the institutions is considered as the institutional solution here. The effectiveness will be evaluated in terms of whether it reinstates access to the systems and data, is easy to implement and the financial cost is low. The impression of how long the initiative was lost, is also a factor. As the attacker's ransom and institutions' guidance are opposing solutions an increase in the trust in the former may reduce trust in the latter:

H9: The perceived effectiveness of the institutional solution to the RW attack will increase the victim's intention to follow institutional guidance.

H10: The perceived effectiveness of the institutional solution to the RW attack will decrease the victim's perceived effectiveness of adopting the ransom solution.

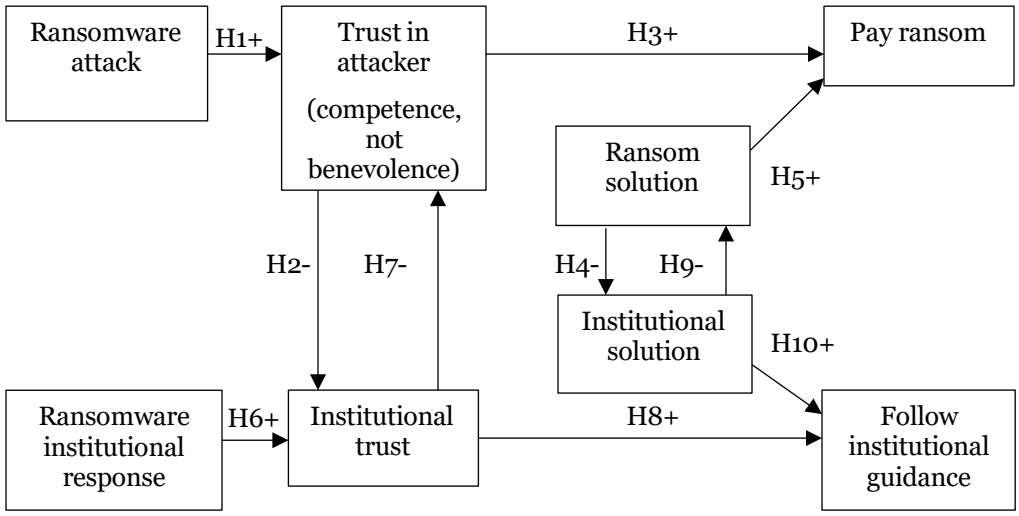

Figure 1. Proposed model of the victim's decision to pay the ransom or follow institutional guidance

Methodology

The epistemological approach was critical realist as there was the event of the RW attack but there were also the victims' beliefs on this event. Given that some aspects of this topic such as how these attacks happen are well understood but other aspects like the impact of global RW attacks are less understood, empirically validating the model was necessary.

A survey was used to evaluate the users' beliefs on the ten hypotheses. Existing scales from the areas of trust, information security, and attitudes towards IS were used where possible (McKnight et al. 2002; Polites and Karahanna 2012; Venkatesh et al. 2003). For each item, a seven-point Likert scale was utilized ranging from strongly disagree (1), to strongly agree (7). There were eight latent variables in total. For six of the latent variables there were four items. For the two latent variables to pay the ransom or follow the guidance three items were used. Three items are considered sufficient for the variable or variables that are the conclusion of a path model (Polites and Karahanna 2012; Venkatesh et al. 2003). Twelve interviews were carried out to evaluate the survey questions in terms of how understandable they were and whether they covered the issues intended. The participants had been victims of RW attacks.

For this model the popular method of estimating the minimum sample size by multiplying the items by ten (Chin and Newsted 1999) would suggest a sample size of 380. The survey was disseminated online to a general sample with 448 respondents. Participants were required to confirm that they had been affected in some way by the RW attacks before they were allowed to access the survey. Participants were asked about their knowledge of the attacks and how the attacks and the response, influenced their beliefs on trust. From these responses 407 were considered complete and valid.

Due to the complex model and need to evaluate latent variables through formative indicator variables the Structural Equation Method (SEM) was used. Covariance based SEM was applied with IBM AMOS 25. Covariance based SEM was selected over Partial Least Squares SEM because this research is primarily confirmatory while allowing exploration of emerging relationships (Hair et al. 2014). Both the measurement model and the structural model were evaluated with the Maximum Likelihood method. The measurement model expresses the relationship between the manifest variables and the latent variables while the structural model expresses the relationship between the latent variables.

Results

The quantitative analysis consisted of a survey to validate the model developed from the literature and refined with the qualitative analysis. The demographic analysis presented in table 1 did not reveal any significant results but it supports that the sample was suitably diverse. Many SEM analysis techniques were applied, and the main findings are presented here.

Demographic profile	Frequency	Percentage
Gender		
Male	178	43.7
Female	226	56.3
Age		
<18	0	0.0
18-30	208	51.1
31-40	151	37.1
>40	48	11.8

Table 1. Profile of the respondents

Measurement model

Several criteria were used to evaluate the formative measurement model. The analysis of the measurement model is presented in table 2 in terms of variance, standardized regression weight, standard error, critical ratio, probability level and mean. The standardized regression weights support the effect of the items on the latent variable. The low standard errors indicate a low spread and that the sample mean is close to the population mean. The critical ratios were above 1.96 and therefore indicated a significant covariance (Hox and Bechger 2009). The statistical significance (P) of all the indicators ($p<0.01$) suggests that the measurement model fit can be considered acceptable (Hair et al. 2014). Lastly the item mean indicates that participants on average agreed with the importance of the issues identified in these items. Overall, the results support the measurement model.

Scale/Item	Variance	S.R.W.	S.E.	C.R.	P	Mean
Ransomware attack	2.242		.225	9.975	***	4.03
RA01		.832	.029		***	
RA02		.823	.027		***	
RA03		.847	.053		***	
RA04		.828	.040		***	
Trust in attacker (competence, not benevolence)	2.423		.238	10.171	***	3.58
TA01		.841	.048		***	
TA02		.821	.041		***	
TA03		.828	.049		***	
TA04		.804	.043		***	

Table 2a. Measurement model measures and results

Scale/Item	Variance	S.R.W.	S.E.	C.R	P	Mean
Ransom solution	1.817		.198	9.179	***	3.22
RS01		.821	.043		***	
RS02		.803	.038		***	
RS03		.834	.055		***	
RS04		.820	.052		***	
Pay ransom	2.144		.221	9.704	***	3.72
PR01		.826	.016		***	
PR02		.816	.015		***	
PR03		.876	.035		***	
Ransomware institutional response	1.292		.157	8.227	***	3.57
IR01		.751	.049		***	
IR02		.689	.034		***	
IR03		.756	.073		***	
IR04		.725	.067		***	
Institutional trust	1.343		.161	8.329	***	3.51
IT01		.757	.068		***	
IT02		.742	.062		***	
IT03		.739	.070		***	
IT04		.698	.054		***	
Institutional solution	1.109		.144	7.708	***	3.50
IS01		.725	.070		***	
IS02		.676	.061		***	
IS03		.729	.081		***	
IS04		.663	.061		***	
Follow institutional guidance	1.293		.161	8.025	***	3.84
IG01		.751	.021		***	
IG02		.743	.020		***	
IG03		.846	.054		***	

***p < 0.01; **p<0.05; *p<0.1

Table 2b. Measurement model measures and results

Structural model

Three of the hypotheses, hypothesis 4, the effect of RS on IS, hypothesis 7, the effect of IT on TA and hypothesis 10, IS on IG were not supported. For hypothesis 4, the effect of RS on IS, the results were S.R.W=0.009, and P=0.516. For hypothesis 7, the effect of IT on TA, the results were S.R.W=0.086, and P=0.323. For hypothesis 10, the effect of IS on IG the results were S.R.W=0.076, and P=0.348. This also led to the original proposed model having an insufficient fit with the data.

The model was further explored by removing these rejected hypothesized effects. Such modifications to a model on empirical grounds are a suitable approach when applying SEM methods (Raykov and Marcoulides 2006; Schumacker and Lomax 2010). The model with the remaining seven relationships was supported by the data. The model supported empirically can also be supported theoretically as all the latent variables were retained and the most important relationships were also retained. The main results of the model are presented in table 3 in terms of standardized regression weight, standard error, critical ratio and probability level. The sample covariance and implied covariance, as indicated by the chi-square value suggest an acceptable fit for the model. The relative/normed chi-square ($\chi 2/df$) was at 4.8 which is below the acceptable ratio of 5.0 (Hooper et al. 2008; Wheaton et al. 1977). A complementary measure of model fit, the root-mean-square error of approximation (RMSEA)=0.077, is also acceptable for this model with these degrees of freedom and this number of participants (Hair et al. 2014). The other measures such as the statistical significance of all the indicators ($p<0.1$), also suggest the model fit can be considered acceptable (Hair et al. 2014).

Hypothesized parameter	Standardized Regression Weight	S.E.	C.R.	P
RA→ TA	.918	.037	31.969	***
TA→IT	.102	.011	3.649	*
TA→PR	.691	.024	17.240	***
RS→PR	.723	.031	16.639	***
IR→IT	.898	.041	28.211	***
IT→IG	.658	.031	14.004	***
IS→IG	.753	.037	15.158	***

Model fit: df= 375, $\chi 2/df$ =4.8, CFI = .929, RMSEA= .0.77; ***p < 0.01; **p<0.05; *p<0.1

Table 3. Structural model measures and results

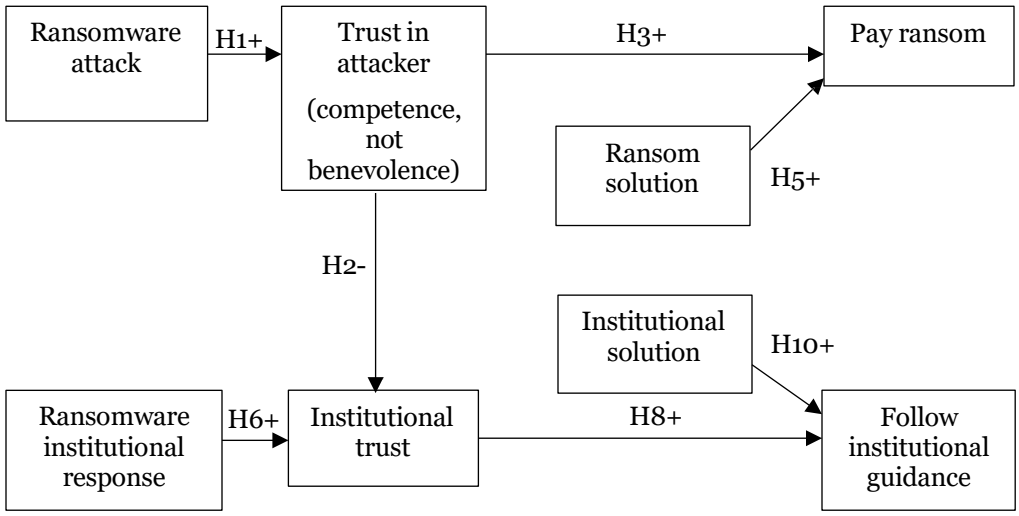

Figure 2. Validated model of the victim's decision to pay the ransom or follow institutional guidance

Discussion and Conclusion

The first target of the RW attacks are the organizations that are held at ransom. Drawing from the literature, a second target of some of the attacks are the institutions that support trust, such as public and private

regulators. In both cases, one dimension of the damage caused is the loss of trust from the users, consumers and patients. This loss of trust influences the decision whether to pay the ransom. If the ransom is paid, this may encourage further RW attacks and create a negative feedback loop of falling trust and a positive feedback loop of increased incentive to make these attacks. It is therefore useful to extend our understanding of the relationship between RW attacks and trust.

Firstly, this research validates the role of trust in the user's, consumer's or patient's decision to pay the ransom or follow the alternative solution offered by the institutions, such as the technology vendors and regulators. Secondly, some factors that influence the intention to pay the ransom were identified. It was shown, that trust in the competence of the attacker influences the intention to pay. The ransom proposed by the attacker should not be seen just as an amount of money. Given that the process of paying the ransom includes the payment method, which is new to most victims, the ransom should be seen as a new technology that must be adopted. Thirdly, some factors that influence the intention to follow the solution offered by the institutions were identified. These included the value offered by the initial response and the institutional trust. The solution proposed should also be seen as a technology being adopted because of its novelty to the user. Fourthly, the interrelationship between the trust in the attacker and the trust in the institutions was proven although this relationship is more limited than what was initially hypothesized. The trust in the attacker's competence has a negative effect on the institutional trust, although this had the weakest effect of all the relationships in the model.

The limitations of this research are that the sample required the participants to have had direct experience of the RW attacks. While the attacks were broad and did not target a specific demographic, this may have biased the sample in a way that was not predicted.

REFERENCES

Aliakbarlou, S., Wilkinson, S., Costello, S. B., and Jang, H. 2017. "Client Values within Post-Disaster Reconstruction Contracting Services," *Disaster Prevention and Management: An International Journal* (26:3), pp. 348–360. (https://doi.org/10.1108/DPM-03-2017-0058).

Chin, W. W., and Newsted, P. R. 1999. "Structural Equation Modeling Analysis with Small Samples Using Partial Least Squares," in *Statistical Strategies for Small Sample Research*, R. Hoyle (ed.), Sage Publications, pp. 307–341.

Erridge, T. 2016. "Ransomware: Threat and Response," *Network Security* (2016:10), pp. 17–19. (https://doi.org/10.1016/S1353-4858(16)30097-6).

Hair, J., Gabriel, M., and Patel, V. 2014. "AMOS Covariance-Based Structural Equation Modeling (CB-SEM): Guidlines on Its Application as a Marketing Research Tool," *Brazilian Journal of Marketing* (13:2), pp. 44–55. (https://doi.org/10.5585/remark.v13i2.2718).

Hooper, D., Coughlan, J., and Mullen, M. 2008. "Structural Equation Modelling : Guidelines for Determining Model Fit Structural Equation Modelling : Guidelines for Determining Model Fit," *Electronic Journal of Business Research Methods* (6:1), pp. 53–60. (https://doi.org/10.1037/1082-989X.12.1.58).

Hox, J. J., and Bechger, T. M. 2009. "An Introduction to Structural Equation Modeling," *Family Science Review* (11), pp. 1–17. (https://doi.org/10.1080/10705510903008345).

Jarvenpaa, S. L., Tractinsky, N., and Saarinen, L. 1999. "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *Journal of Computer-Mediated Communication* (5:2), Blackwell Publishing Ltd, p. 0. (https://doi.org/10.1111/j.1083-6101.1999.tb00337.x).

Khokhar, R. H., Fung, B. C. M., Iqbal, F., Alhadidi, D., and Bentahar, J. 2016. "Privacy-Preserving Data Mashup Model for Trading Person-Specific Information," *Electronic Commerce Research and Applications* (17), Elsevier B.V., pp. 19–37. (https://doi.org/10.1016/j.elerap.2016.02.004).

Mayer, R. C., Davis, J. H., and Schoorman, F. D. 1995. "Model of Trust," *Academy of Management* (20:3), pp. 709–734.

McKnight, H., Choudhury, V., and Kacmar, C. 2002. "Developing and Validating Trust Measures for E-Commerce : An Integrative Typology," *Information Systems Research* (13:3), pp. 334–359.

Mercaldo, F., Nardone, V., and Santone, A. 2016. "Ransomware inside out," in *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, pp. 628–637. (https://doi.org/10.1109/ARES.2016.35).

Mustaca, S. 2014. "Are Your IT Professionals Prepared for the Challenges to Come?," *Computer Fraud and Security* (2014:3), Elsevier Ltd, pp. 18–20. (https://doi.org/10.1016/S1361-3723(14)70472-5).

Orman, H. 2016. "Evil Offspring - Ransomware and Crypto Technology," *IEEE Internet Computing* (20:5),

pp. 89–94. (https://doi.org/10.1109/MIC.2016.90).
Pavlou, P. A. 2003. "Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model," *International Journal of Electronic Commerce* (7:3), pp. 69–103. (https://doi.org/10.1.1.86.7139).
Pavlou, P. A., and Gefen, D. 2004. "Building Effective Online Marketplaces with Effective Institution Based Trust," *Information Systems Research* (15:1), pp. 37–59.
Polites, G. L., and Karahanna, E. 2012. "Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance," *MIS Quarterly* (36:1), pp. 21–42.
Raykov, T., and Marcoulides, G. A. 2006. "A First Course in Structural Equation Modeling," *Structural Equation Modeling: A Multidisciplinary Journal* (Vol. 13), New Jersey: Lawrence Erlbaum Associates. (https://doi.org/10.1207/s15328007sem1301).
Schumacker, R. E., and Lomax, R. G. 2010. "Multiple Indicator-Multiple Indicator Cause, Mixture, and Multilevel Models," *A Beginner's Guide to Structural Equation Modeling*. (https://doi.org/10.1002/9781118133880.hop202023).
Simmonds, M. 2017. "How Businesses Can Navigate the Growing Tide of Ransomware Attacks," *Computer Fraud and Security* (2017:3), Elsevier Ltd, pp. 9–12. (https://doi.org/10.1016/S1361-3723(17)30023-4).
Simon, F., Clare, B., and Nan, Z. 2009. "Web-Based Group Decision Support for Crisis Management," *International Journal of Information Systems for Crisis Response and Management (IJISCRAM)* (1:1), pp. 41–53. (https://doi.org/10.4018/jiscrm.2009010104).
Song, J., and Zahedi, F. M. 2007. "Trust in Health Infomediaries," *Decision Support Systems* (43:2), pp. 390–407. (https://doi.org/10.1016/j.dss.2006.11.011).
Thatcher, J. B., McKnight, H., Baker, E. W., Arsal, R. E., and Roberts, N. H. 2011. "The Role of Trust in Postadoption IT Exploration: An Empirical Examination of Knowledge Management Systems," *IEEE Transactions on Engineering Management* (58:1), pp. 56–70. (https://doi.org/10.1109/TEM.2009.2028320).
Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly* (27:3), pp. 425–478.
Wecksten, M., Frick, J., Sjostrom, A., and Jarpe, E. 2016. "A Novel Method for Recovery from Crypto Ransomware Infections," in *IEEE International Conference on Computer and Communications*, pp. 1354–1358.
Wheaton, B., Muthen, B., Alwin, D. F., and Summers, G. F. 1977. "Assessing Reliability and Stability in Panel Models," *Sociological Methodology* (8), p. 84. (https://doi.org/10.2307/270754).
Zarifis, A., Efthymiou, L., Cheng, X., and Demetriou, S. 2014. "Consumer Trust in Digital Currency Enabled Transactions," *Lecture Notes in Business Information Processing* (183), pp. 241–254. (https://doi.org/10.1007/978-3-319-11460-6_21).