Your Money or Your Business: Decision-Making Processes in Ransomware Attacks

Short Paper

Lena Yuryna Connolly
University of Bradford
Department of Computer Science

Richmond Road, Bradford, UK
l.yurynaconnolly@bradford.co.uk

Hervé Borrion
University College London
Department of Security and Crime Science
35 Tavistock Square, London, UK
h.borrion@ucl.ac.uk

Abstract

In this paper, we explore decision-making processes of ransomware victims, focusing on organisations. We examine 39 ransomware attacks using qualitative data collected from victims and police officers from cybercrime units in the UK. A basic premise of this paper is that victims make rational decisions to (not) pay ransoms. Their decision-making processes represent a complex infrastructure that consists of several reasons that drive these choices. Our research shows that victims weigh the costs and benefits of the attack outcomes before making final decisions. The aim of this work is to develop an in-depth understanding of these processes and suggest measures to avoid ransom payments, which, in turn, will help reduce ransomware crime.

Keywords: Ransomware attacks, Rational Choice Theory, organisations, decision processes

Introduction

In their annual Internet Organised Crime Threat Assessment report, Europol (2019) identified ransomware as the main malware threat to organisations and predicted this trend would continue over the coming years. With the average ransom payment gradually increasing from about $300 in 2015 to $36,000 in the second quarter of 2019, ransomware is now a lucrative criminal business that accounts for over $11 billion of the cost of cybercrime (Korolov 2017, Sjouwerman 2019). Among victims, many organisations reported having paid amounts that significantly exceeded the average ransom cost. As an example, Nayana, a South Korean web hosting company is notorious for having paid $1 million, one of the largest ransoms ever recorded, in exchange for a decryption key for its servers (Chirgwin 2017). Major ransoms were also paid by local governments including Jackson County, Georgia ($400,000) and the city of Riviera Beach, Florida ($600,000) (Ferguson 2019a, 2019b). Huang et al. (2018) traced financial transactions from the moment victims acquire bitcoins to when ransomware operators cash them out and tracked over $16 million in likely ransomware payments made by 19,750 potential victims during 2016 and 2017. In their global survey of 540 organisations, Malwarebytes (2016) found that 37% of ransomware victims paid ransom in 2016. As ransomware becomes a major risk to organisations globally, the need to defeat it is greater than ever.

Ransomware is a complex phenomenon that involves two types of crime: hacking and cyber extortion. Both crimes must be successful for offenders to reap a financial reward:

Hacking, the technological part, starts with the infiltration of a network via exploitation of human or software vulnerabilities, then proceeds with the ransomware propagation within the network and subsequent encryption of critical data, which in turn may lead to disabled systems vital for business continuity. Plentiful research has been conducted on hacking. Scholars and practitioners provided advice on how to prevent ransomware from penetrating networks (Simmonds 2017) and spread within (Mansfield-Devine 2018). Al-rimy et al. (2018) stressed that although data recovery is unlikely if asymmetric cryptography is employed, further developments in the field of cryptanalysis (i.e., a process of deciphering coded messages without a key) is a promising avenue for victims to regain access to the files without paying the ransom. Connolly and Wall (2019), however, argued that there is no simple technological solution to defeat the ransomware threat. Rather, a multi-layered approach is needed which consists of socio-technical measures, zealous front-line managers and active support from senior management.

Cyber extortion, also referred to as 'digital extortion', involves informing victims of the extent of damage, ransom demand and the consequences of not paying it. Typically, this phase of a ransomware attack focuses on a psychological manipulation of victims to pay ransom. In contrast to hacking, empirical research on cyber extortion in the context of ransomware is much more limited. In fact, we only found one publication analysing this phase of the crime commission process using empirical data. Using game theoretic models, Cartwright et al. (2019) viewed extortion as a form of kidnapping of victim's files and concluded that the bargaining power of the criminals lies within the victim's willingness to recover their files, the likelihood of the offender to destroy files if a ransom demand is not met, and the credible commitment to return files to a victim who pays the ransom.

The rise of ransomware can arguably be explained by a cost-benefit equation. Indeed, the fact that targeted individuals and organisations agree to pay ransoms makes it a profitable business. In order to break what could be described as a vicious circle, a better understanding of how victims decide whether to pay a ransom is needed. For this, we are currently analyzing 39 ransomware incidents in an attempt to shed light on the factors that influence the payment of ransoms. Specifically, we aim to understand whether the Rational Choice Theory (RCT) framework so often used in criminology is 'good enough' to explain victims' decisions (Cornish & Clarke, 2003). The following section presents the framework along justifications as to why we adopted it for this study. The focus of this paper is solely on *crypto-ransomware*. This is because since around 2013, cybercriminals have almost exclusively deployed this type of ransomware to extort money as opposed to alternatives such as *scareware*, *lockers* and *wipers* (Hull et. al., 2019).

Theoretical Framework

Rational Choice Theory

Originated during the late 18th century with the work of Cesare Beccaria and Jeremy Bentham, RCT has been extensively used to represent, understand and sometimes predict social and economic behaviour (Geis 1955, Blume and Easly 2008). The RCT school of thought is based on the assumption that individuals are so-called 'rational agents' who take into account available information, probabilities of events, and potential costs and benefits in determining preferences and act consistently in choosing actions that best achieve their goals and objectives (Hogg and Jennings 1997). The rational perspective, therefore, is often used to formally model the process of human decision making. In its essence, the theory focuses on the determinants of the individuals' choices (Uzonwanne 2016).

In the field of criminology, Walters (2015) stated that the version of RCT that received most attention and empirical support is the *Reasoning Criminal* perspective proposed by Cornish and Clarke (1985). This approach hypothesises that offenders' decisions to commit crime are informed by a cost-benefit analysis, and that crime is more likely to occur if the perceived benefits are high and the perceived costs are low (Piquero and Hickman, 2002). While the rational choice approach cannot be considered a perfect explanatory model of crime (N.B: this point is discussed below), Cornish and Clarke (1985) regarded it as 'good enough', in that it allows situational factors of crime to be identified and organised to support the development of crime reduction interventions, including against organised crime (see Cornish & Clarke 2003).

The rational choice perspective was supported through surveys and interviews with offenders. Gill and Matthews (1994), for instance, found that crime prevention strategies afford the opportunity to intervene at various stages in the development of robberies and as a consequence deflect or dissuade potential offenders. O'Grady et al. (2000) identified factors that influence merchants' decisions to illegally sell tobacco to underage youth. Corbett and Simon (1992) studied decision-making processes of individuals who engage or refrain in traffic offences. Varma and Doob (1998) applied RCT in order to understand the effect of criminal justice sanctions on tax evasion. Beauregard and Leclerc (2007) investigated the decision-making involved in the offending process of sexual offenders and concluded that even impulsive and irrational sex offenders are capable of a cost-benefit analysis related to their actions.

Wright (2010) argued that the rational perspective is also suitable to study cybercrime (not only terrestrial crime) and factors that motivate or discourage cybercriminals to commit online offences. Modarres et al. (2013) stressed that RCT is relevant to cybercrime and subsequently examined motivations of cybercrime from the offender's perspective. Bachmann (2010) found that hackers show a strong preference for rational decision-making processes. Rege (2014) focused on cyber attacks in the energy sector and concluded that adversaries are rational actors that conduct thorough research before executing these attacks. Guitton (2012) revealed that rational hackers who are concerned about the socio-economic cost of the punishment and have sufficient knowledge about the attribution processes (i.e. investigation, arrest and prosecution of individuals who intrude or disrupt networks), respond to deterrent mechanisms. Rege (2016) discovered that understanding the adversarial decision-making processes is imperative in better profiling cybercriminals and effectively deploying resources to counter advanced persistent threat attack on critical infrastructure. All of these studies support the main postulation that criminals, including cyber offenders, weigh benefits and costs when making a decision whether to commit a crime or not.

RCT has been predominantly employed to examine offender decision-making. More relevant to the problem investigated in our work, a small number of studies have applied RCT to the decisions made by potential targets of crime (Borrion 2013). Smith (2009), for instance, examined how risk perception and fear of crime influence pedestrians' trajectories when walking in the street. Supporting the RCT framework, her results suggest that personal security concerns have a critical effect on the victims' decisions to alter their trajectory. Hong and Neilson (2018) considered a situation with a rational victim, a rational hacker, and a social planner (e.g. government) and concluded that the victims' investment in security combined with potential fines may or may not deter the hacker from attempting the crime in the first place. More specifically, if the penalty for committing crime is increasing, the potential victim becomes complacent and invests in security less, increasing the success probability of crime. A rational hacker only pays the fine if the crime is unsuccessful, therefore the attacker avoids punishment by committing the crime successfully. The more the rational victim invests in security, the more effort the hacker makes to commit successful crime. Meyer (2012) examined the decision-making processes of domestic violence victims to stay with their partners despite the abuse and identified factors that influence these choices. The same approach is arguably applicable to understand the factors that influence targets' decision to pay a ransom.

Rational Choice Theory and Cyber Extortion

While the RCT approach offers the advantage of simplicity and practicality, there is no evidence that it explains victims' decisions in cyber extortion cases. Indeed, the assumption that human behavior is in line with individual preferences has many opponents (Camerer et al. 2011). In her study of domestic violence, for example, Sivitz (2014) called for future research on the decision-making processes of domestic violence victims to adopt more complex models taking into account cognitive biases (e.g., availability heuristic and sunk cost bias). Researchers have also challenged the use of rational choice theory to explain offender behaviour. In the field of Situational Crime Prevention, for example, Wortley & Tilley (2017) have recently argued that 'rational choice assumptions are implausible and unnecessary'.

These criticisms may, however, not be as strongly applicable to financial decisions made by organisations (Carter 1971, Nilsson and Dalkmann 2001). Indeed, organisations' decisions to pay ransoms are arguably the result of careful economic and risk considerations rather than emotional responses. Furthermore, there is anecdotal evidence that offenders expect victims to take rational decisions as they go to great lengths to convince them that paying the ransom is in their best interests. The literature mentions techniques such as warning the victim of the consequences of not paying the ransom; setting a strict deadline by which it should be paid with the threat to destroy all files after the deadline passes; offering to decrypt one file to prove the ownership of the decryption key; making a credible commitment to return the files to the victim who pays the required ransom; introducing an escalated payment system (e.g. an earlier payment would entail a discount); delivering excellent customer service to deal with the purchase of bitcoins and other issues; informing the victim about the vulnerabilities that need to be patched up to avoid further cyber attacks (Conti et al., 2018; Cartwright et al., 2019; Connolly and Wall, 2019). Another important aspect to consider is that decision-making models need not be perfect to be useful. Clarke, for example, often referred to RCT as a “good enough” model for the purpose of crime reduction (Cornish and Clarke 2003, Smith and Clarke 2012).

Methods

Case Studies

The study examined 39 purposely selected ransomware attacks that happened between 2014 and 2018. Cases where selected to show a diversity of organisations, potential outcomes and payment decisions. The selected sample comprises 34 organisations, including 23 small and medium enterprises (SMEs) and 11 large enterprises (LE). Among them, 16 were classified as public sector and 18 as private sector organisations. In total 16 industry sectors were represented in the dataset including law enforcement, government, education, health, information technology (IT), construction, infrastructure, religion, entertainment, utilities, cleaning, waste, logistics, transport, charity, and retail. Table 1 is an illustrative representation of relevant demographic data of organisations participated in this research study. Considering that the victim’s decisions are potentially influenced by the expected outcomes of a ransomware attack, we selected attacks with various consequences, ranging from low severity (e.g. minimum disruption to business, minimum loss of information, swift recovery) to high impact (e.g. business disruption that lasted for several months, significant loss of critical information, slow recovery). Consequence estimation was performed using the Impact Assessment Instrument (IAI) (Connolly et al., 2020). The IAI was inductively developed from data collected for the aforementioned study and used to evaluate the severity of crypto-ransomware incidents on organisations that became victims of these attacks. We intentionally used cases representing a balanced set of outcomes.

Case ID	Organisation alias	Industry; size; sector
1	LawEnfJ	Law enforcement; SME; Public
9	LawEnfM	Law enforcement; SME; Public
10		
11	GovSecA	Government; LE; Public
20	ITOrgJL	IT; SME; Private
35	LogWarJ	Logistics; LE; Private

Table 1. An Illustrative Subset of Participating Organisations

The Ethics Committee at the University of [REMOVED FOR REVIEW] approved this research. Consent forms were signed by all study participants. All necessary precautions were followed to ensure the anonymity of participants and the confidentiality of collected data. The majority of participants (i.e. victims) were from the UK but there were also a few from North America. Where the names of organisations are subsequently referred to in this paper, aliases have been used to protect the anonymity of respondents (see Table 1). Additionally, interviewees from UK Police Cybercrime Units are given the aliases of CyberRM, CyberLM, CyberTL and CyberBR.

Data Collection

Different methods were used for data collection. Semi-structured interviews with 11 ransomware victims were conducted, producing data on 16 cases (some victims were attacked more than once). We interviewed 10 participants in person and online (Skype); and emailed 1 participant due to their very busy schedule. Interviewees were IT/Security Managers and Executive Managers with an average of 17 years of professional experience. All of them had direct experience of responding to ransomware incidents.

The shortcomings of interviewing victims directly were, however, swiftly realised: it was exceptionally difficult to find organisations willing to share information about their victimisation experience. Therefore, we decided to take a different approach and contacted police officers from UK Cybercrime Units who had direct experience of dealing with ransomware victims, more specifically UK organisations. When responding to ransomware attacks, Cybercrime Units in the UK conduct an in-depth investigation of these incidents, which involves prolonged conversations with the victim company representatives (especially when victims are considering payment). Police help victims counter ransomware attacks, provide emotional support to victims, advise on measures to avoid further attacks, and even deliver post-breach security awareness training in some instances. Such deep involvement affords police officers an opportunity to spend prolonged periods of time with organisations and develop a deep understanding of the attacks as well as consequences for the victims. As a Detective Sergeant from CyberTL put it:

> "*I would argue that no other group of people have a more in-depth understanding of the motivations of the attackers, the varying methods by which the attacks are executed and the impact on victims than the police.*"

The expectation was that each police officer would be able to share data on several incidents at the time and have the ability to provide information on decision-making processes of ransomware victims. We contacted 8 police officers (two Detective Sergeants and six Detective Constables) and one Civilian Cybercrime Investigator with the average professional experience of 19 years. Data was collected via semi-structured interviews and one focus group and 23 further cases were added to the existing 16. Two police officers were interviewed twice because they were able to add information on new cases.

Interviews lasted between 30 and 135 minutes. We began our interviews with an open-ended question asking interviewees to share information about ransomware attacks they had experienced. We then proceeded by deeply probing into each attack to elicit more detailed information including: how the attack occurred, whether ransom was paid or not and why, consequences of the attack etc. We concluded the interviews by asking participants to add any relevant details they would like to share.

Data Analysis

A *framework analysis* method was used for this study. Initially developed for applied policy research (Ritchie and Spencer, 1994), it has since been adopted in other research domains and has become an established method for qualitative data analysis (Furber, 2010). Framework analysis is a *case-and-theme* based approach that aims to reduce the data via summarisation and use a matrix to represent the results of the analysis linked to the original data. It differs from more traditional qualitative data analysis techniques (e.g. content analysis) as the focus is not on 'coding' data but rather 'synthesising' it in a form of matrix. This is a particularly useful method to meet the objectives of this study because the synthesis utility allowed us to address the complexity of the data. More specifically, victims' decision-making processes (not) ti pay were based on multiple reasons each. These included primary and secondary reasons, with the added complexity that what was a primary reason for one victim could be a secondary for another and *vice versa*.

Data analysis was performed in five successive phases. In Phase 1 (Familiarisation), interview transcripts were read several times in order to make sense of the data and construct draft narratives of each case. This exercise demonstrated that the reasons behind victims' decisions (not) to pay are complex and, in many cases, multiple motives and trade-offs drove victims' choices. Phase 2 (Identifying Themes) involved breaking the data down into themes. We divided ransomware attack cases into two main themes such as "Paid Ransom" (n=7) and "Did Not Pay Ransom" (n=32). Phase 3 (Coding) entailed the coding of fragments of data, where several sub-themes emerged under each theme defined in Phase 2. More specifically, we identified 10 reasons 'to pay ransom' and 20 reasons 'not to pay ransom' (Table 2 represents an illustrative subset of Phase 3 themes).

Phase 2 Themes	Paid Ransom	Did not Pay Ransom
Phase 3 Themes and relevant Code IDs	1.Ineffective backups 2.Encrypted data was critical to business continuity 4.The victim came close to bankruptcy 10.As per IT consultants' advice	1.Effective backups 2.Encrypted data was not critical to business continuity 3.As per authorities' advice 19.Unsuccessful negotiation 20.Unethical to facilitate crime

Table 2. An Illustrative Subset of Phase 3 Themes

In Phase 4 (Summarising), we formed 15 unique 'information containers', each containing a unique set of reasons (not) to pay the ransom relevant to one or more cases (Table 3). We wrote a detailed description (or summary) for each container, each of which signified a unique decision-making process. This was the most time-consuming phase of data analysis, as it required repeatedly returning to the transcripts for verification. During this phase, summaries were iteratively modified until we were completely satisfied with the accuracy and completeness of the results. Finally, in Phase 5 (Matrix Building), we identified corresponding *case(s)* (i.e. rows in matrix that represented ransomware attack) and *codes* (i.e. columns in the matrix that represented a unique set of reasons behind each decision-making process) for each information container. We built two matrices: one comprising the cases where victims paid the ransom and the other where victims refused to pay. Table 3 illustrates one ‘information container’ from each matrix. Matrices not only help visualisation of results but also guide results reporting and link results to data, making it easy to retrieve any evidence.

“Paid Ransom”		“Did Not Pay Ransom”	
	Code ID: 1, 2 and 4		***Code ID***: 3
Case IDs: 20, 35	Business operations solely relied on digital data (private organisation). When ransomware stroke, critical data got encrypted and all vital operations were ceased. Backups were not available. The victim made a decision to pay the ransom to avoid bankruptcy.	***Case ID***: 11	A public organisation suffered an unprecedented attack, where around 100 servers got encrypted, disabling several important services. The victim only had partial backups. They immediately reported the incident to authorities and were subsequently advised not to pay the ransom. Upon reflection, the organisation regretted not to explore a possibility of paying to offenders as recovery was extremely challenging (over a year). If it was a private organisation, the business would not survive.

Table 3. An Illustration of Information Containers from Each Matrix

Preliminary Results Trustworthiness

Several methods were used to establish the trustworthiness of data analysis results. First, we employed tactics to ensure honesty in participants. We clearly explained our approaches to ensure anonymity and confidentiality. Furthermore, interviewees were informed that they could withdraw from the study at any time and refuse to answer questions deemed inappropriate. For example, some participants, when describing the incidents, could not reveal systems’ vulnerabilities that led to the attacks as this information could potentially make victims vulnerable to subsequent attacks. Second, all interview transcripts were sent to study participants to avoid any errors and misinterpretations. Third, upon reading the transcripts, some context was not immediately clear, and we held follow-up conversations with participants to clarify our own interpretations.

Remaining Work

Preliminary results show that decision-making processes of ransomware victims represent a complex structure and will have to be interpreted with caution. Therefore, in the next phase of the study, we intend to organise a brain-storming exercise with academic fellows to discuss our case studies and preliminary findings. We will look for at least one expert in ransomware research and one expert in qualitative research. If anything was overlooked in data or missed out during data analysis, we expect this discussion will address these limitations. Next, based on the results, we expect to develop techniques that could potentially reduce ransom payments. To ensure the proposed measures are feasible, we intend to organise a workshop with police officers from UK cybercrime units. We expect to discuss topics such as the implementation of the proposed measures in practice, the dissemination of the measures among potential victims etc. We envisage that police will add important insights to our work. We also plan to organise another workshop with security professionals from potential victim organisations to get a more valid and direct representation of their decision-making perspectives. This would not necessarily be drawn from organisations that had already been victimised, but would relate to people who are or should be actively considering the issues at stake, and the measures.

Acknowledgements

We would like to extend our sincere gratitude to all respondents for their invaluable contribution to this research. We greatly appreciate interviewees' time and genuine effort. We are very grateful for additional inputs during and after data analysis; the comments and corrections provided invaluable contribution in shaping findings.

We would like to acknowledge the relentless commitment of Police Officers from UK's regional CCUs in providing data and advising on study results.

This work was supported by the Engineering and Physical Sciences Research Council via two grant schemes: EMPHASIS (EconoMical, PsycHologicAl and Societal Impact of RanSomware) [EP/P011721/1] and ACCEPT (Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks) [EP/P011896/1].

Please note that the views expressed in this work are ours alone and do not necessarily reflect those of the participants, the commentators or the funding body.

References

Al-rimy, B.A., Maarof, M.A., Shaid, S.Z.M. 2018. "Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions", *Computers & Security* (74), pp. 144-166.

Bachmann, M. 2010. "The Risk Propensity and Rationality of Computer Hackers", *International Journal of Cyber Criminology* (4:1&2), pp. 643-656.

Beauregard, E. and Leclerc, B. 2007. "An Application of the Rational Choice Approach of the Offending Process of Sex Offenders: A Closer Look at the Decision-Making", *Sex Abuse* (19), pp. 115-133.

Blume, L.E. and Easly, D. 2008. "The New Palgrave Dictionary of Economics", 2nd Edition. Palgrave, Macmillan. [Online] Available at: https://link.springer.com/referencework/10.1057/978-1-349-95121-5 [Accessed 11th October 2019].

Borrion, H. 2013. "Quality assurance in crime scripting", *Crime Science* (2:6), pp. 1-12.

Camerer, C.F. and Loewenstein, G. 2003. "Behavioral Economics: Past, Present, Future", in: *Advances in Behavioral Economics*, C.F. Camerer, G. Loewenstein, G. and M. Rabin (eds.), Princeton University Press, pp.3-52.

Caporusso, N., Chea, S. and Abukhaled, R. 2019. "A Game-Theoretical Model of Ransomware", in: *Advances in Human Factors in Cybersecurity*, T.Z. Ahram and D. Nicholson (eds.), SpringerLink, pp. 69-78.

Carter, E.E. 1971. "The behavioural theory of the firm and top-level corporate decision", *Administrative Science Quarterly* (16:4), pp.413-429.

Cartwright, E., Hernandez Castro, H. and Cartwright, A. 2019. "To Pay or Not: Game Theoretical Models of Ransomware", *Journal of Cybersecurity* (5:1), pp. 1-12.

Chirgwin, R. 2017. "South Korean hosting co. pays $1m ransom to end eight-day outage", The Register, 20 June. [Online] Available at: https://www.theregister.co.uk/2017/06/20/south_korean_webhost_nayana_pays_ransom/ [Accessed 15th September 2019].

Connolly, L. and Wall, D. 2019. "The Rise of Crypto-Ransomware in a Changing Cybercrime Landscape: Taxonomising Countermeasures", *Computers & Security* (87), pp. 1-18.

Connolly, L., Wall, D. and Lang, M. 2020. "An Empirical Investigation of Ransomware Attacks on Organisations: An Assessment of Severity and Salient Factors Affecting Vulnerability", *Research Gate*, [Online] Available at: https://www.researchgate.net/publication/340537050_An_empirical_study_of_ransomware_attacks_on_organisations_an_assessment_of_severity_and_salient_factors_affecting_vulnerability (Preprint version).

Conti, M., Gangwal, A. and Ruj, S. 2018. "On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective", *Computers & Security* (79), pp. 162-189.

Corbett, C. and Simon, F. 1992. "Decisions to Break or Adhere to the Rules of the Road, Viewed from a Rational Choice Perspective", *British Journal of Criminology* (30:4), pp. 537-549.

Cornish, D.B. and Clarke, R.V. 1985. "Modeling Offenders' Decisions: A Framework for Research and Policy", in *Crime and Justice: An Annual Review of Research*, M. Tonry and N. Morris (eds.), Illionis: University of Chicago Press (6), pp. 147-185.

Cornish, D.B. and Clarke, R.V. 2003. "Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention", in *Theory for Practice in Situational Prevention*, M.J. Smith and D.B. Cornish (eds.), London: Criminal Justice Press and Willian, pp.41-96.

Europol 2019. "Internet Organised Crime Threat Assessment 2019", Report, Europol. [Online] Available at: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018 [Accessed: 11th September 2019].

Ferguson, S. 2019a. "Florida city paying $600,000 to end ransomware attack", Bank Info Security, 20 June. [Online] Available at: https://www.govinfosecurity.com/florida-city-paying-600000-to-end-ransomware-attack-a-12673 [Accessed 11th September 2019].

Ferguson, S. 2019b. "Georgia County pays $400,000 to ransomware attackers", Bank Info Security, 12 March. [Online] Available at: https://www.bankinfosecurity.com/georgia-county-pays-400000-to-ransomware-attackers-a-12159 [Accessed 11th September 2019].

Geis, G. 1955. "Pioneers in Criminology VII--Jeremy Bentham (1748-1832)", *Journal of Criminal Law. Criminology & Police Science*, (46:2), pp. 159-171.

Gill, M. and Matthews, R. 2005. "Robbers on Robbery: Offenders' Perspectives", in *Crime at Work,* M. Gill (ed.), London: Palgrave Macmillan.

Guitton, C. 2012. "Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence", *International Journal of Cyber Criminology* (6:2), pp. 1030-1043.

Hogg, L.M. and Jennings, N.R. 1997. "Socially Rational Agents", *AAAI Fall Symposium on Social Intelligent Agents*, pp. 61-63.

Hong, Y. and Neilson, W. 2018. "Cybercrime and punishment: a rational victim model", Working Paper. [Online] Available at: http://abbyhong.com/wp-content/uploads/2017/08/Cybercrime-and-Punishment-A-Rational-Victim-Model-5.pdf [Accessed 13th December 2019].

Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., McRoberts, K., Bursztein, E., Levin, J., Levchenko, K., Snoeren, A.C. and McCoy, D. 2018. "Tracking ransomware end-to-end", in *Proceedings of the IEEE Symposium on Security and Privacy 2018*, pp. 618-631.

Hull, G., John, H. & Arief, B. 2019. "Ransomware deployment methods and analysis: Views from a predictive model and human responses", *Crime Science*, (8:2), pp. 1-22.

Korolov, M. 2019. "Report: Average ransomware demand now over $1000", CSO, 3 May. [Online] Available at: https://www.csoonline.com/article/3193981/report-average-ransomware-demand-now-over-1000.html [Accessed 10th October 2019].

Malwarebytes 2016. "Understanding the Depth of the Global Ransomware Problem". [Online] Available at: https://www.malwarebytes.com/pdf/whitepapers/UnderstandingTheDepthOfRansomwareIntheUS.pdf [Accessed 3rd November 2019].

Mansfield-Devine 2018. "The malware arms race", *Computer Fraud and Security* (2), pp. 15-20.

Meyer, S. 2012. "Why Women Stay: A Theoretical Examination of Rational Choice and Moral Reasoning in the Context of Intimate Partner Violence", *Australian and New Zealand Journal of Criminology* (45:2), pp. 179-193.

Modarres, M., Mandelcorn, S. and Mosleh, A. 2013. "An Explanatory Model of Cyber-Attacks Drawn from Rational Choice Theory", *American Nuclear Society Meeting on Risk Management for Complex Socio-Technical Systems*, Washington, United States, 12-14 June.

Nilsson, M. and Dalkmann, H. 2001. "Decision Making and Strategic Environment Assessment", *Journal of Environmental Assessment Policy and Management*, (3:3), pp.305-327.

O'Grady, W., Asbridge, M. and Abernathy, T. 2000. "Illegal Tobacco Sales to Youth: A View from Rational Choice Theory", *Canadian Journal of Criminology* (1) pp. 1-20.

Piquero, A.R. and Hickman, M. 2002. "The Rational Choice Implications of Control Balance Theory", in *Rational Choice and Criminal Behavior,* A.R. Piquero and S.G. Tibbetts (eds.). New York: Routledge.

Rege, A. 2014. "A Criminological Perspective on Power Grid Cyber Attacks: Using Routine Activities Theory and Rational Choice Perspective to Explore Adversarial Decision-Making", *Homeland Security & Emergency Management* (11:4), pp. 463-487.

Rege, A. 2016. "Incorporating the Human Element in Anticipatory and Dynamic Cyber Defense", in *Proceedings of the IEEE International Conference on Cybercrime and Computer Forensic 2016*, pp.1-7.

Ritchie, J. and Spencer, L. 1994. "Qualitative Data Analysis for Applied Policy Research", in *Analyzing Qualitative Data*, A. Bryman and R.G. Burgess (eds.). New York: NY: Routledge, pp. 173-194.

Sjouwerman, S. 2019. "Ransomware attacks cost nearly triple in 2019 to over $36K per attack", KnowBe4, 24 July. [Online] Available at: https://blog.knowbe4.com/ransomware-attacks-costs-nearly-triple-in-2019-to-over-36k-per-attack [Accessed 12th September 2019].

Simmonds, M. 2017. "How businesses can navigate the growing tide of ransomware attacks", *Computer Fraud & Security* (3), pp. 9-12.

Sivitz, E. 2014. "Rational Choice and Domestic Violence: How Decision Theory can Inform Domestic Violence Policy", *Student Perspectives on Institutions, Choices & Ethics* (9:1), pp.48-91.

Smith, M.J. 2009. "A Six-Step Model of Potential Victims' Decisions to Change Location", *Security Journal* (22:3), pp. 230-249.

Smith, M and Clarke R. (2012) "Situational Crime Prevention: Classifying Techniques Using 'Good Enough' Theory", in *The Oxford Handbook of Crime Prevention*, B.C. Welsh and D.P. Farrington (eds.) Oxford University Press, pp.291-315.

Varma, K.N. and Doob, A.N. 1998. "Deterring Economic Crimes: The Case of Tax Evasion", *Canadian Journal of Criminology* (40), pp. 165-184

Uzonwanne, F. 2016. "Rational Model of Decision Making, in *Global Encyclopedia of Public Administration, Public Policy, and Governance*, A. Farazmand, (eds.), New York: Springer, pp. 1-6.

Walters, G.D. 2015. "The Decision to Commit Crime: Rational or Nonrational?" *Criminology, Criminal Justice Law & Society* (16:3), pp. 1-18.

Wortley, R.K and Tilley, N. 2017. "Does situational crime prevention require a rational offender?", in: *The Future of Rational Choice for Crime Prevention*, D.M. Reynald and B. Leclerc (eds.), Routledge, pp. 8-27.

Wright, C.S. 2010. "Criminal Specialization as a Corollary of Rational Choice", *Social Science Research Network Electronic Library*. [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3461064 [Accessed 11th November 2019].