Computers & Security 119 (2022) 102760

Contents lists available at ScienceDirect

Computers & Security

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

Reducing Ransomware Crime: Analysis of Victims' Payment Decisions

Alena Yuryna Connolly*, Hervé Borrion

Zayed University, Liberty Building, Leeds, United Arab Emirates

ARTICLE INFO

Article history:
Received 5 June 2021
Revised 18 February 2022
Accepted 16 May 2022
Available online 25 May 2022

Keywords:
Ransomware attacks
Organisations
Decision processes
Ransom payments
Cybercrime

ABSTRACT

In this paper, the decision-making processes of victims during ransomware attacks were analysed. Forty-one ransomware attacks using qualitative data collected from organisations and police officers from cybercrime units in the UK were examined. The hypothesis tested in this paper is that victims carefully analyse the situation before deciding whether to pay a ransom. This research confirms that victims often weigh the costs and benefits of interventions before making final decisions, and that their decisions are based on a range of reasons. As ransomware attacks become more prevalent globally, the findings should be highly relevant to those developing guidance and policies to prevent or minimise ransom payments.

1. Introduction

In their annual Internet Organised Crime Threat Assessment report, Europol (2020a) 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 $111,605 in 2020, ransomware is now a lucrative criminal business that accounts for over $11 billion of the cost of cybercrime (Bisson, 2020; Morgan, 2020). Among victims, many organisations reported payments well above the average ransom cost. Colonial Pipeline, the largest pipeline system for refined oil products in the United States, is notorious for having paid $4.4 million, one of the largest ransoms ever recorded, in exchange for a decryption key for its systems (Eaton and Volz, 2020). 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. They tracked over $16 million in likely ransomware payments made by 19,750 potential victims during 2016 and 2017. According to Ndichu (2021), 52% of ransomware victims paid ransom in 2020. 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, and continues 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 a ransom. Connolly and Wall (2019), however, argued there is no simple technological solution to defeat ransomware threats. Rather, a multi-layered approach combining socio-technical measures, zealous front-line managers and active support from senior management is needed.

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, only one publication analysing this phase of the crime commission process using empirical data was found. 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 offenders lies within the victim's willingness to recover their files, the likelihood of the offender to destroy files if a

* Corresponding author.
E-mail address: alena.yuryna-connolly@fulbrightmail.org (A. Yuryna Connolly).

https://doi.org/10.1016/j.cose.2022.102760

ransom demand is not met, and the credible commitment to return files to a victim who pays the ransom.

Arguably, the rise of ransomware can be explained by profitability of this crime. Indeed, the fact that targeted individuals and organisations agree to pay ransoms makes it an attractive business. In order to break what could be described as a vicious circle, it is useful to gain a better understanding of the decision making process during an attack. For this, 41 ransomware incidents in an attempt to shed light on the factors that influence the payment of ransoms were analysed. The focus of this paper is solely on *crypto-ransomware* 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).

2. Methods

2.1. Case studies

The study examined 41 purposely selected ransomware attacks that have occurred between 2014 and 2018. As shown in Appendix A, cases were selected to include a diversity of organisations. The sample comprises 36 organisations: 24 small and medium enterprises (SMEs) and 12 large enterprises (LE). Of those, 15 were classified as public sector and 21 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. Considering that the victim's decisions are potentially influenced by the expected outcomes of a ransomware attack, 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) were selected. Consequence estimation was performed using the Impact Assessment Instrument (Connolly et al., 2020). This instrument 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. Cases representing a balanced set of outcomes were intentionally selected.

2.2. Data collection

Different methods were used for data collection. Semi-structured interviews with 11 ransomware victims were conducted, producing data on 16 cases. Ten participants in person and online (Skype) and emailed 1 participant due to their busy schedule were interviewed. 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 were, however, swiftly realised: it was very difficult to find organisations willing to share information about their victimisation experience. Therefore, it was decided to take a different approach and contact 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 representatives of the victimised company. 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 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. Eight police officers (two Detective Sergeants and six Detective Constables) and one Civilian Cybercrime Investigator with the average professional experience of 19 years were contacted. Data was collected via semi-structured interviews and one focus group, and 25 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 min. Interviews began with an open-ended question asking interviewees to share information about ransomware attacks. Next, it was necessary to deeply probe into each attack to elicit more detailed information including: how the attack occurred, whether ransom was paid or not and why, and what the consequences of the attack were. Interviews were concluded by asking participants to add any relevant details they would like to share.

2.3. 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 to address the complexity of the data. More specifically, victims' decision-making processes (not) to pay were based on multiple reasons. These included primary and secondary reasons, with the added complexity that what constituted a primary reason for one victim could be a secondary for another.

Data analysis was performed in five successive phases (Fig. 1).

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. Ransomware attack cases were initially divided into two main themes such as "Paid Ransom" ($n = 8$) and "Did Not Pay Ransom" ($n = 33$). A detailed examination of cases revealed that the identified themes are too broad to fully reflect the complexity of decisions made by victims and, therefore, must be further broken down into sub-themes (Table 1).

Phase 3 (Coding) entailed the coding of fragments of data that represent the reasons victims made decisions to (not) pay ransom. A close examination of these codes revealed that they fall into three broad categories: ***available information*** (codes 1–29), where victims assess the immediate damage and recovery prospects; ***probabilities of events*** (codes 30–39), where victims evaluate the prospects of events relevant to business continuity and ***potential***

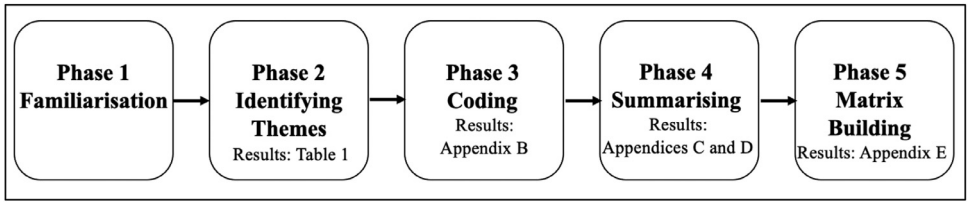


Fig. 1. The phases of data analysis.

Table 1
Results of phase 2 (Identifying Themes and Sub-Themes).

Themes	n	Sub-Themes
Paid Ransom;	1	Ransom paid by IT provider
$n = 8$	3	Real threat of bankruptcy
	1	Inability to recover intellectual property
	2	Inability to recover criminal data
	1	Fear of incrimination
Did Not Pay	22	Had no intention to pay
$n = 33$	7	Considered payment
	2	Wanted to pay but could not afford
	1	Shabby IT provider – potential link with offenders
	1	The decision not to pay was later regretted

costs and benefits (codes 40–64), where victims analyse the advantages and disadvantages of (not) paying the ransom (Appendix B). Essentially, before determining actions to pay or not (Phase 2 sub-themes), victimised organisations conducted meticulous cost-benefit analysis using all available information about the attack and its potential consequences.

Furthermore, the reasons (not) to pay could be labelled as primary or secondary reasons, although the same reason could be seen as primary for one victim and secondary for another. Appendix B contains all relevant information from phase 3 data analysis.

In Phase 4 (Summarising), 23 unique 'information containers' (17 where victims did not pay the ransom and 6 where victim did) were formed, each containing a unique set of reasons (not) to pay the ransom relevant to one or more cases (Appendices C and D). A detailed description (or summary) for each container, each corresponding to a unique decision-making process was written. This was the most time-consuming phase of data analysis, as it required repeatedly returning to the transcripts for verification. During this phase, Phases 2 and 3 were continuously refined and summaries were iteratively modified until the accuracy and completeness of the results reached the highest possible level.

Finally, in Phase 5 (Matrix Building), *case(s)* (i.e., rows in matrix that represented ransomware attack) were cross-referenced with *information container(s)* (i.e., columns in the matrix that represented a unique set of reasons behind each decision-making process). Appendix E illustrates the results of Phase 5. Matrices not only help visualisation of results but also guide results reporting and link results to data, making it easy to retrieve any evidence.

The Ethics Committee at the [University Removed] approved this research. Consent forms were signed by all participants. All necessary precautions were followed to ensure the anonymity of participants and the confidentiality of collected data. Most participants were from the UK, with a few others 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 Appendix A). Additionally, interviewees from UK Police Cybercrime Units are given the aliases of CyberRM, CyberLM, CyberTL and CyberBR.

3. Results and discussion

Data analysis results were meticulously examined for victims' decisions to (not) pay ransoms. Some of these decisions were very complex and had multiple variables at play, including primary and secondary. Dominating reasons to (not) pay were used as sub-headings in this section. Other decisions included several reasons with similar characteristics, and it made sense to report them under a common umbrella (i.e., sub-heading High Level of Preparedness incorporates variables such as *effective backups*, a *clear incident response strategy* and a *full network visibly*). All in all, ten principal sub-headings have emerged as a result of this exercise, forming Results and Discussion section.

3.1. High level of preparedness

Recommendations are routinely made for individual organisations to prevent and prepare against ransomware attacks (Europol, 2020b; Interpol, 2020 and NCSC, 2020). The consequences of not following this advice were perhaps best exemplified in the case of SecOrgM, a private business, that was faced with a very large ransom and no opportunity to pay or negotiate (i.e., the victim wanted to pay, but hackers did not leave any contact details). Critical data and systems got encrypted and the organisation did not have backups. SecOrgM went out of business as a result of this attack.

GovSecA, another victim that wanted to pay ransom, had experienced an unprecedented attack due to poor level of preparedness. As an IT Manager shared:

> "*The picture I am going to paint for you is that it was Tuesday morning after the August bank holiday weekend, and the sun was streaming in through the windows, the cleaners have been in, the office looked great. Everyone felt refreshed and everyone felt good after the long holiday. And it took quite a while for us to realise what had happened. That everything, all the computing had been turned to stone. Everything. Nothing, virtually nothing was left untouched. So, nothing worked, everything was just dead.*" (Security Manager, GovSecA)

GovSecJN, an organisation that refused to pay the ransom, had a very tough recovery due to flaws in the incident response strategy. Following an ineffective initial response, ransomware had a chance to spread, making recovery more difficult.

Police provided the following comment on the topic of successful recovery:

> *"Ransomware is so prevalent because of weak security practices. You cannot be perfect all the time. But if you have certain things at 95% or even 90%, you might take a hit, but you are at least going to recover". [Detective Constable, CyberBR]*

At the other end of the spectrum, several cases were identified where not only targeted organisations were able to successfully recover from ransomware, but the recovery was both swift and straightforward. Study participants acknowledged that effective backups, clear incident response strategy, and a full visibil-

ity of infected systems and the network are important factors that contributed towards the decision not to pay a ransom. As one of the victims noted:

> "*We were much better prepared second time around. We knew how to respond to the attack. We also had effective backups, which allowed us to recover most of the data"* (Executive Police Officer, LawEnfM, 2nd attack)

Admittedly, not all victims that implemented the aforementioned measures had a swift recovery. HealthSerJU was attacked twice within a few months. Issues like ineffective patching regime and out-of-date anti-virus (AV) allowed ransomware to spread to hundreds of devices. Some ransomware variants have advanced propagation capability and hence require organisations to implement additional measures. For instance, Generation III ransomware takes advantage of poor authentication controls, flat network structure, insufficient patching, as well as the lack of network visibility and detection mechanisms (Connolly et al., 2020). Similarly, InfOrgJL and TranspOrgJ had effective backups, clear incident response strategy and network visibility, but because ransomware spread to too many devices, the victims struggled with recovery.

Interestingly, two victims, VirtOrgD and CloudProvJL, had effective backups in place but still considered payment. Upon a thorough examination of the situation, they estimated that the recovery time from a decryption key would be as time consuming as from backups. If a decryption key had sped up their recovery, they would have paid to reduce the substantial business loss incurred on a daily basis.

3.2. Playing Russian Roulette with Ransomware

Despite having a poor level of preparedness, several organisations were simply fortunate. Ransomware encrypted data that was critical to LawEnfJU's business continuity (i.e., criminal evidence). The victim instantly hired external consultants who managed to find a decryption key for this particular ransomware variant. Subsequently, LawEnfJU did not pay. Although this is an option that needs to be always explored by the victims, generally, cybercriminals replace obsolete variants relatively fast. Besides, the usability of the decryption tools (particularly provided by NoMoreRansom project) needs to be improved, and decrypting data using these tools could be challenging.

Although the encrypted data was critical to business continuity for ConstrSupA, ConstrSupJ and SportClubJ, these businesses had a small window of opportunity to recover as business could only function for several days before collapsing. For instance, ConstrSupA lost sensitive data, which disrupted their operations. However, the business was not fully digitised, and the company was able to restore most of its data via printed paper copies. As one of police officers noted:

> *"They did not pay because of the way their business worked; the attack did not have a big impact on them. So, if you go to tech-based business…They have everything online, and everything digitised. And such an attack would have a detrimental effect on them. But slightly old-fashioned companies…I suppose I can call them that…Would not be as affected." [Detective Constable, CyberTL]*

ConstrSupJ, however, was not as fortunate: ransomware crippled accounting system and 6 years of financial data was lost. While most crucial data was swiftly recovered via collaboration with various company's stakeholders, it took months for ConstrSupJ to return to 'business-as-usual'. In the meantime, several partners broke contracts with the victim due to unpaid bills. ConstrSupJ received countless complaints from customers. Essentially, the company was on the verge of collapse. Some important data was never recovered.

Finding alternative recovery paths beyond backups is, undeniably, very inventive on victims' part. Indeed, all recovery avenues should be explored and taken advantage of. Playing Russian roulette with ransomware, however, is dangerous. Based on the above scenarios, it is reasonable to recommend the implementation of data classification schemes. Once the organisations know their most valuable assets, they need to protect them accordingly. One of the problems that many organisations have been regularly facing though is not knowing their data, which makes it impossible to protect it (Maniatis et al., 2011). Knowing data locations, especially in large organisations, is no small task. EducInstFB was faced with similar problem post-attack. One of the reasons the victim decided to pay is because they did not know what data was actually missing due to the lack of network visibility in some areas:

> *So right or wrong, and it is still something we are working on, we have a fairly significant number of sub-networks of our network that were not managed by IT. We had no control over upgrading or updating the operating systems, virus definitions…overall, very limited visibility. So really it was like a fog…we knew that computers were plugged into network nodes, but we could not see them…And we did not know what sort of data then was encrypted. So that was really our biggest challenge. [Executive Manager, EducInstFB]*

Connolly and Wall (2019) acknowledged that managing networks, especially of a large size, is difficult. On the other hand, security breaches have become more sophisticated, and attackers are keen to target as many machines as possible on a network. Ransomware has gone through successive evolutionary steps, ranging from the first ever recorded attack in 1989 by the variant that could not propagate beyond an infected machine to highly sophisticated types coined as 'Generation III' and 'Generation IV' that are capable of paralysing large networks and even travel beyond a single organisation (Connolly et al., 2020, 2021). Indeed, the complexity of networks have been increasing with the technological advances and innovations. The lack of visibility, however, is leaving organisations struggling to identify network data and investigate suspicious network activity tied to malicious attacks. Security actors are increasingly exploiting this weakness as they prefer to stay undetected (Miller, 2020). Organisations are urged to identify blind spots in their networks and account for each device and piece of data. Once blind spots are discovered, it is necessary to document and classify assets and provide appropriate level of security throughout the whole network. Connolly and Wall (2019) advise virtualisation as one of the potentials solutions to issues related to network visibility, but, at the same time warn of security issues in cloud environments.

3.3. Risk of bankruptcy

Private organisations must remember that they would normally feel the pain of ransomware attacks much more severely than those in the public sector, with bankruptcy being a very realistic outcome (Connolly et al., 2020). As mentioned above, one of the private companies in the dataset, SecOrgM, went bankrupt. The victim did not have backups and the ransom was too high, with no opportunity to negotiate. Several other victims came very close to bankruptcy.

Two servers of ITOrgA, a small private IT company, were brute forced via weak Remote Desktop Protocol (RDP) passwords. As a result, the victim lost access to critical data and systems, which completely froze business operations. Due to poor backups, ITOrgA did not have even the slightest chance of recovery, but a very real threat of bankruptcy. Such extreme consequences forced the victim to pay the ransom. Fortunately for the victim, the offenders hon-

oured their promise on the delivery of the decryption key. One of the police officers shared the following details about the attack:

> *"It was kind of a supply chain company in the IT sector and clients really depended on certain deliverables. A number of customers were waiting on deadlines for the work that the company was doing. The Director was a day away from missing those deadlines and not being able to function." [Detective Sergeant, CyberRM]*

ITOrgJL is another small private IT company that came very close to bankruptcy. This was a highly organised attack. Ransomware penetrated victim's network and snooped around until full recon was conducted. Perpetrators found backups, deleted them, and only then encrypted valuable data. The ransom note, however, did not include the ransom amount but rather attackers' email address with the invitation to contact them. Following a very thorough assessment of the situation, ITOrgJL initiated communication with extortionists. The attackers asked for 100 bitcoins, which was an unrealistic amount to pay. ITOrgJL started a negotiation, which went over several days – attackers acted like they were very reluctant to reduce the ransom. During the negotiation, they even threatened the victim with the GDPR fines. When the ITOrgJL complained that the amount is too large for such small business, offenders replied that the victim holds 250 terabytes of data and has a large number of servers and customers, indicating prosperous business operations and hence the ability to pay. Such detailed information on victim's resources indicates thorough recon. Nevertheless, the victim managed to prove that 100 bitcoins was not a manageable amount for them. Subsequently, the ransom was reduced. ITOrgJL paid the ransom and successfully decrypted all resources. During first few days of the attack, the victim was not sure if they would survive. Customers sent a flood of complains and some even left.

LogWarJ is a large logistics business that got infected due to the weak RDP password. Similar to the ITOrgJL attack, perpetrators stayed on the network undetected while conducting recon. Attackers discovered several vulnerabilities that allowed ransomware to spread on hundreds of machines (including backups), crippling the whole network. Since the victim did not have any offsite backups and the business could not possibly survive without the encrypted resources, they paid a relatively large ransom in an exchange for the decryption key. Subsequently, LogWarJ managed to restore most of their data. This was an exceptionally severe attack that could easily have cost LogWarJ their business.

Ransomware can have major financial implications for victims (Zhang-Kennedy et al., 2018; Zhao et al., 2018). Although this is true for all organisations, commercial entities can also be at risk of bankruptcy. Connolly et al. (2020) found that private organisations were more likely to experience serious negative consequences as a result of a ransomware attack compared to public organisations. This is because private organisations are mainly operating for profit and financial losses hit them hard. Subsequently, it is reasonable to urge private businesses to up their game and strengthen their security position in order to avoid the prospect of bankruptcy.

3.4. Type of data

Information is another reason why victims pay ransoms to extortionists.

EducInstFB, an educational institution, suffered an unprecedented attack. Ransomware crippled the network of hundreds of machines, and encrypted large amounts of data including research data and findings. Such disruption can prevent researchers to meet project deadlines and affect future relationships with collaborators and funding bodies. Loss of research outputs can also affect an HEI's intellectual property and revenue stream. In the extreme, it can cause an HEI to drop in international league tables, affecting the number and calibre of academic staff and students.

LawEnfF and LawEnfM (first attack) lost information that was crucial to criminal investigations. Backups were not available. Implications of losing this data could be very serious:

> *"I was told that we have not lost anything… Data was only encrypted…The thought of somebody having a copy of the child sex investigation would have been unbearable. But we are a full-service law enforcement agency, and we do anything from manslaughter cases, child pornography, child sex cases. So, there is a lot of sensitive data there that got encrypted and would have been lost if we did not pay… So that really was not a good option for us." [Executive Police Officer, LawEnfM]*

Ransomware actors are aware that for successful extortion it is best to encrypt *valuable* data. As the dataset suggests (e.g., EducOrgA, RelOrgJ, CleanOrgD, EducOrgD, ServOrgD, EducCompD, PrimOrgD, CharOrgJ, and EducInstJ), targeted organisations are perhaps less likely to pay when non-critical data is encrypted, even if the victim does not have backups (e.g., CleanOrgD).

As ransomware continually advances its technical capabilities, its attack tactics evolve. In 2013, when ransomware actors started making considerable profits, 'spray-and-pray' attacks dominated (Connolly and Borrion, 2020). At the time and up around until 2016, offenders aimed to attack as many victims as possible and asked for a relatively affordable ransom. Since around 2016, it seems that the modus operandi has changed and attacks became more targeted – perpetrators were choosing victims according to their ability to pay (Connolly et al., 2020). Once inside the network, attackers implemented tools that allowed them to propagate on the network and find valuable data. Accordingly, perpetrators started asking for much higher bounties in an exchange for a decryption key. As was already mentioned in Section 2, organisations are urged to develop and implement data classification schemes and apply defence mechanisms appropriate for the level of data sensitivity.

3.5. Fear of incrimination

Fear of incrimination by data protection authorities was found an important factor in the decision to pay ransoms. Despite having implemented effective backups, PrivCoJL paid ransom out of fear of being persecuted by the information commissioner's office. Attackers stole sensitive data and demanded ransom in return for their silence. The victim could easily restore data if it was only encrypted, but they made a decision to pay, hoping that the breach would never be discovered. As one of the police officers shared:

> *"One of the methods ransomware actors operate is that they will infiltrate your network, copy your data and put it somewhere else. Then they will send you a message saying, 'We have your data, come and see your data. If you do not pay us money, we will release data.' We have seen attackers even sending victims GDPR Wikipedia page and saying, 'If you do not get this sorted out, you will get fined'. It is like offenders are using law enforcement against victims." [Detective Constable, CyberTL]*

FinOrgJL is another victim whose confidential data was copied and transferred to the attackers' location. Offenders did not encrypt any resources. The victim received an email from attackers notifying them of the breach and the consequences of not paying. Essentially, perpetrators threatened to sell data on the Dark Web. They also provided credentials to access part of the victim's data as evidence that they hold it. At the time, FinOrgJL had thousands of customers whose personal data was affected. Offenders never provided the ransom amount – instead the expectation was that the victim will contact them first. Indeed, this would indicate

that the victim is ready to pay. Although FinOrgJL was tempted to pay, they decided against it. The victim was afraid to become a target of indefinite blackmail as there was no guarantee offenders would then delete the stolen data. FinOrgJL decided to inform all customers of the breach. This attack took place in 2018 before the GDPR came into force. Therefore, FinOrgJL did not have the same pressure of reporting the incident to the Information Commissioner Officer (ICO).

3.6. Fear of secondary victimisation

DigMedM did not pay out of fear of secondary victimisation. The victim was a small start-up company, and if they were to pay ransom, they would have to take a loan due to very tight budget. Indeed, they considered this option. DigMedM also tried to negotiate the ransom amount down, but unsuccessful. After difficult deliberations, the director decided to recover from ineffective backups. The logic behind this decision was simple – if the offenders decided to ask for a second ransom, they would not survive. DigMedM were afraid to be perceived as an easy target if they pay. Instead of paying, DigMedM decided to invest into security and close down all loopholes. FinOrgJL had similar concerns and was afraid to be added on offenders' 'sucker list'. One of police officers shared with the following:

"We always tell victims, 'If you pay, criminals might not give you a decryption key. There is always risk of that. They will take your money or your bitcoin, and they might expect more. Once you paid, you are on a 'sucker list'. And you can get targeted again – they might expect another payment. We cannot tell victims whether to pay or not, but we can tell them potential consequences." [Detective Constable, CyberBR]

Indeed, this is a very real problem, and victims need to take in consideration such scenario if they decide to pay. Offenders who normally intend to give victims a decryption key are also aware of this trend. Essentially, this is damaging for their business. Therefore, perpetrators try hard to convince victims that they are 'honourable' thieves (e.g., sending very convincing emails, or a decryption key to decrypt a portion of data). EducInstFB and LawEnfM had similar concerns, but external consultants reassured the victims otherwise:

"The breach coach made it clear that we do not have any ability to negotiate as we were only given 72 h to pay…It is a tactic to avoid negotiation…One thing we did though is we asked for 'proof of life key' to ensure that the criminals had the ability to decrypt our data. They sent us a decryption key to decrypt a portion of our data. At least we knew they have the ability. The breach coach also advised that the package deal [one master key to decrypt hundreds of devices for once-off payment] was a pretty sweet deal. We were also told that normally criminals release the key because, if they do not, other cybercriminals would be very upset with them as it impacts their commerce…interestingly enough there is some level of honour amongst thieves." [Executive Manager, EducInstFB]

Naturally, my initial reaction was, 'We are not going to engage with criminals, we are not going to be held hostage. I am a cop' But my IT folks right away said, 'You should pay this. We have had similar situations with out clients. And these guys [this particular criminal gang] have some level of integrity. It may sound crazy, but they tend to keep their ransom low, so it is not unattainable, and victim can weigh their options. All our previous victims received a decryption key. Criminals hold true to their word. You give them money, they give you the key, and usually you have little or no damage at the of the day'." [Executive Police Officer, LawEnfM]

The bottom line is that victims need to take in consideration advice from police and external consultants, evaluation all options, and make an optimal business decision whether to pay or not.

3.7. Ransom amount

The amount the criminals asked for also had an impact on victims' decision to (not) pay. UtilOrgD was asked to pay an amount of 75 bitcoins. The company could not afford such large ransom and tried to negotiate. The criminals, however, were very reluctant to reduce it. The negotiation reached an impasse, and the victim decided to recover data from partial backups. HealthSerJU did not even attempt a negotiation as over a thousand of devices got encrypted on both incidents. The victim simply predicted that the ransom would be too high:

"We did not pay the ransom because over a thousand of machines were infected. We thought we would be asked to pay an awful lot of money" [Security Manager, HealthSerJU]

LawEnfM and LawEnfF, on the other hand, commented that the ransom was relatively inexpensive, which could potentially impact victims' decisions:

"When we found the ransom note, we concluded that it was relatively inexpensive, which I think is part of the lure for the perpetrators of the crime. They are pretty clever on their part in this sense. They only wanted $350 for a decryption key" [Executive Police Officer, LawEnfM]

As was mentioned earlier, ITOrgJL was asked for 100 bitcoin ransom – the amount they would not be able to pay. At the same time, the victim would go out of business without the decryption key. ITOrgJL initiated a very aggressive negotiation. At first, cybercriminals were reluctant to reduce the ransom. But once the perpetrators realised that the victim genuinely could not afford such big ransom, they agreed to drop the amount. Ultimately, offenders preferred to receive some bounty rather than walk away with nothing. As one of the police officers shared:

"ITOrgJL received an initial demand for 100 bitcoins. They could not afford to pay it, but the business survival was dependent on the decryption key. So, the victim negotiated over a period of 3 days, it was a very intense negotiation. They went back and forward emailing, emailing and emailing to criminals. And it worked." [Detective Constable, CyberTL]

Generally, data demonstrate that if the ransom is too high, victims will attempt recovery without paying. In some instances, however, organisations cannot survive without the decryption key and, therefore, are cornered into a tough negotiation (e.g., ITOrgJL). SecOrgM was not given an opportunity to negotiate and went bankrupt. Indeed, different organisations have different abilities to pay. What considered to be a very high ransom for one organisation, could be perceived as an acceptable amount for another. Hackers endeavour to get it right and even employ business models to assess the optimal ransom amount (Connolly and Wall, 2019). In order to evaluate the victims' ability to pay, ransomware attacks are becoming more targeted. Cybercriminals conduct a thorough recon on networks to estimate the optimal amount as was the case with ITOrgJL.

3.8. Incorrect advice

GovSecA – a public organisation – suffered an unprecedented attack, where around 100 servers got encrypted. Subsequently, several critical services were disabled and data important to business continuity was encrypted. Having only partial backups and poor

incident response strategy, the victim predicted a difficult recovery. Seeking help, they immediately reported the incident to authorities and were subsequently advised not to pay the ransom as the amount would be too high due to the number of infected machines. Upon reflection, the organisation learned that they could have tried to negotiate the amount of the ransom and possibly pay for a master key that would have decrypted all machines. The organisation regretted not exploring the possibility of paying the ransom as recovery proved extremely challenging and took over a year. It must be noted that a private organisation would not survive such an attack. This is why, while the general advice from law enforcement agencies is to avoid paying a ransom, police also observe that the decision must be considered in a broader context:

> "*We are police, so we cannot really tell organisations to make or not to make that payment. It is their business decision*." *[Detective Constable, CyberBR]*

In the case of the GovSecA attack, law enforcement agents did not have sufficient knowledge to provide adequate advice regarding a master decryption key. Perceiving authorities as incompetent in dealing with cyber breaches can potentially discourage reporting. Additionally, wrong decisions could lead to severe and irreversible consequences for the victims. Indeed, cybercrime is still relatively new territory for police. Taking in consideration that cybercrime is continuously evolving and there is an acute shortage of cybersecurity skills (Virgo, 2021), it must be incredibly difficult to 'play catch up' game. Dodd (2020) notes that constant cuts to police budget further exacerbate the matter. In line with the Competency and Values Framework (CVF) authored by the College of Policing (2016), we argue that police competency in dealing with cyberattacks must be improved and advice regarding payments must be relevant and accurate. HMICFRS (2019) conducted a national inspection into police response to cyber-dependent crimes in UK and found several areas that require urgent improvements, including enhancing knowledge about cybercrime, prioritising of cybercrime, and distributing of resources according to the type of cyber incident.

3.9. Feeling responsible for the attack

In some instances, parties that feel responsible for the attack may pay the ransom.

LawEnfM was attacked by ransomware twice within two weeks. In the first instance, ransomware encrypted data critical for criminal investigations. Since the victim did not have backups, they decided to pay. In the meantime, their external IT provider assisted with recovery as well as with the measures to prevent further attacks and backups. Unfortunately, the victim was hit by ransomware a second time and critical data was encrypted again. Although backups were available, the IT provider felt responsible for this breach and decided to pay. Due to the punctual nature of backups and level of sensitivity of encrypted data, they thought it was best to decrypt all the data:

> *"The second time we would be able to rebuild that data. But our IT provider actually paid the ransom. We did not pay it because we were fine. But the IT provider wanted to get back certain data; and they felt a level of responsibility. It happened so close to the first attack, so they paid. So, the second time we were able again to decrypt data in its entirety. And we moved on." [Executive Police Officer, LawEnfM]*

One would argue that in this instance it was not necessary to pay the ransom. Organisations should only consider payments in exceptional circumstances. If the IT provider recovered data via backups and discovered that something critical was missing, then such decision could be potentially justified. However, paying 'just in case' is unacceptable. Organisations need to remember that with every payment they facilitate cybercrime and encourage perpetrators to conduct further attacks. Indeed, the most effective way to eradicate ransomware is to stop paying.

3.10. Reluctant to facilitate crime

Several victims in the dataset were reluctant to facilitate crime (e.g., LogOrgD, VirtOrgD and FinOrgJL). LogOrgD, a logistics and warehousing company, received a significant demand for payment after a server that contains crucial data was encrypted. Business operations of the victim were fully dependent on the digital data, and backups were not available. LogOrgD realised that they were on the verge of collapse. However, the business owner strongly believed that paying criminals was wrong. As one of the police officers commented:

> *"The director had a strong opinion that it is wrong to finance criminals.* LogOrgD *hired IT specialists to help with recovery. After a swift assessment, the IT company said, 'Listen, you are stuffed now. There is nothing we can do with your backups – they are encrypted. The only avenue for you is to either start again or engage with the criminals.' But the director said, 'I do not want to engage with criminals.' After about five days, customers started leaving and it looked like the company was not going to survive. The director was very upset as he built this business up from scratch, it was his life's work… And he started considering payment…" [Detective Sergeant, CyberTL]*

VirtOrgD's experience with ransomware was also very dramatic, but the director firmly believed that no payment should be made to offenders:

> *It was the managing director's firm belief that the criminals would not receive any bonus whatsoever. He did not want to proliferate criminal activity through funding them. He was very passionate about that. [Detective Sergeant, CyberTL]*

FinOrgJL had a similar stand to VirtOrgD and LogOrgD:

> *"They believed it was an ethical thing. They said, 'Okay, we have been compromised, but if will pay, this will happen again to someone else.' They took a standpoint that it was not right to pay ransom" [Detective Constable, CyberTL]*

Ultimately, all these victims could have paid a ransom to offenders under different circumstances. FinOrgJL's data was not actually encrypted (only stolen), and the victim could continue 'business-as-usual'. They made a hard decision of informing customers. A decryption key would not have saved VirtOrgD from the immediate pain they experienced as a result of the attack. They actually had backups and the decryption key would not speed up a recovery. LogOrgD, while was considering a payment, found a company that was helping victims of ransomware. They paid £5000 to this IT provider. The following day, police discovered that a payment had been made to the bitcoin address offenders provided to LogOrgD for payment. Law enforcement suspected that the IT provider had links with the offenders.

4. Final words

The interviews conducted on ransomware experiences suggest victims often perform some kind of cost-benefit analysis before deciding whether to pay the requested ransom. The victim's capability to pay, both financially and practically, is a major factor in their decision. The main obstacles to payment are when the offender insists on a ransom amount beyond what the victim can afford, and when they fail to provide victims with the information they need to proceed with the payment. Victims may also be dissuaded by

difficulties experienced at other stages of the process (e.g., how to obtain and transfer bitcoins). However, offenders will often provide guidance to overcome these issues and facilitate the transaction.

Among the victims that could pay the ransom, many of them appear to have analysed the advantages and disadvantages of paying offenders against those of i) retrieving encrypted information from alternative means (e.g., obtaining a decryption key from an IT specialist, using digital backups or paper records) or ii) collecting new data from existing customers. Knowing that recovery is rarely complete, quick and easy, many victims will consider paying a ransom even when backups are available, so to can minimise disruption and the risk of further financial loss. To these elements must be added the possibility that offenders make the ransomware public, which can cause significant reputation loss and fines from regulators.

Following a simple cost-benefit analysis, the payment of a ransom can be perceived as the most rational decision. However, the uncertainty about offenders' intent can make the decision-making problem more complex. Indeed, there is a risk that offenders won't provide a decryption key, that they request more money later on, or that they place victims on a 'suckers list', thus facing greater risk of victimisation in future.

Available knowledge and trust can also play an important role in shaping a decision. For example, not all victims know they can engage in negotiation over the amount of the ransom. Also, they may simply follow the advice of a third party and subsequently decide not to pay.

Besides these pragmatic reasons, moral values were sometimes mentioned as having influenced victims' decisions. Some victims voiced that the payment of a ransom was morally wrong, as it financially benefits offenders and encourages them to carry out further attacks. Conversely, a service provider who felt they had not sufficiently reduced the security vulnerability of their client after a first attack decided to pay the ransom after the second one. Besides these anecdotal cases, it is unclear how much morality plays a role in victims' decisions.

Another important point to remember from these interviews is the systemic incentive that organisations have to pay ransoms

Connolly et al. (2021) reported that data theft in ransomware attacks has become particularly prevalent since around 2020 when ransomware stopped bringing expected bounties to perpetrators due to organisations having much stronger security measures in place. This new ransomware, coined as Generation IV, added a blackmail element, preying on victims' fears (i.e., fear of incrimination, fear of reputational damage and lost revenue, fear intellectual property exposure or loss, fear of embarrassment). Several Generation IV ransomware attacks have been confirmed by victims via media statements, including the University of California San Francisco (UCSF, 2021), University of Stanford (UoS, 2021), University of California Berkeley (UCB, 2021). Media reports that some victims made substantial ransom payments to hackers to prevent data leak. For example, the University of California San Francisco paid $1.14 million in bitcoins following data theft and a subsequent ransomware attack (Tidy, 2020). In a similar attack, the University of Utah paid $457,000 to prevent a data leak (O'Donnell, 2020). Uber paid hackers in exchange for a promise to delete 57 million user records and did not report the incident to the authorities (Menn and Stempel, 2020).

One of the interviewees sympathised with victims and suggested to reconsider the incident reporting mechanism enforced by the GDPR and data protection offices in Europe:

> *"Too many cyber incidents are kept quiet because of fear of incrimination. Organisations are afraid of persecution by information commissioners…With GDPR, the cybercriminal no longer has to get the latest crypto technology to beat the government or local services. What they do is infiltrate network and steal a large amount of valuable data. Then threaten the company, 'We will release these to the ICO or publish it to embarrass you'. The fines issued by the ICO are up to 2% of your turnover, which can be millions of pounds, even billions of pounds. Or for ten bitcoins or whatever the amount is [ransom] cybercriminals offer to delete your data from their location. If you go to the ICO and say, 'We have been hacked. We have had data stolen', it is like going to the headmaster and saying, 'I stole that little boy's lollipop, but I am sorry here it is back'. The ICO are still going to fine them. Companies often prefer to pay the ten bitcoins [ransom] and hope that it goes away quietly. So, the ICO have got to rethink and have some mechanism in place to encourage companies to report. Like a parking ticket – if you pay the parking ticket within 14 days, it is only £20 instead of £60. So maybe with the GDPR, they should say, 'If you tell us on day one that it happened, we will be lenient towards you. But if you tell us two weeks later, a month later, whatever later, then you are going to get the full force of the law'. There has got to be some way to take into account the honesty of the organisation. Otherwise, you are creating another problem, by fining them such a huge amount". [Security Manager, GovSec]*

Fear is a powerful emotional response to a perceived threat, and it directly impacts human behaviour (Hazam and Felsenstein, 2006; Cacciotti and Hayton, 2015). Fear is also a strong motivator for people to change their normal behaviour to avert a potentially negative outcome (Chen, 2016). Invoking fear in people is an effective tactic to trigger desired actions (Johnson and Warkentin, 2010). It, however, can also prompt controversial and even unlawful reactions. For instance, Papp et al. (2019) found that fear of retaliation discourages individual's willingness to cooperate with police, even when they believe reporting is the right thing to do. Furthermore, deterrence mechanisms are largely irrelevant to those with little propensity to commit acts of crime. On the other hand, some studies show that reward mechanisms can support compliance (Boss et al., 2009; Bulgurcu et al., 2010). Moreover, Chen et al. (2012) demonstrated that reward enforcement could be an alternative in settings where sanctions do not successfully prevent violation.

The ultimate purpose of the GDPR and other data protection regulations, indeed, is to protect data and rights of individuals to whom this data belongs. If, however, reporting is discouraged due to the exceptionally harsh penalties, there is a need to revisit the current deterrence approach. Rewarding victims' honesty can potentially increase reporting and therefore reinforce the GDPR's commitment to protect individuals' data. Data demonstrates that victims conduct thorough cost benefit analysis before making a decision whether to pay or not. Equally so, it can be assumed that victims weigh costs and benefits before making a decision whether to report the breach or not. If the fine is much greater than the ransom offenders are looking for, victims may choose not to report.

5. Conclusions

Reducing ransomware crime has become a key objective for governments and industry across the world. The findings show there are many reasons why targeted organisations may decide to pay a ransom, even when they have backups. Many of these reasons can be understood through financial analysis, and relate to the effectiveness, speed, difficulty and cost of the recovery, as well as reputational risk and potential fines from regulators. However, the interviews also revealed that less predictable elements that can play an important role in the decision (not) to pay the ransom: lack of knowledge, poor advice, collusion, morality, feeling of responsibility, pressure, uncertainty and trust. These "soft" elements

are potentially key to the development of more effective guidance and policies to reduce ransom payment. More research should be conducted to understand their manifestation and influence in the crime process. Additionally, policies should be reviewed to ensure the current regulatory system does not disincentivise victims to reporting cyberattacks.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper

CRediT authorship contribution statement

Alena Yuryna Connolly: Conceptualization, Methodology, Data curation, Writing – original draft, Investigation, Visualization, Formal analysis. **Hervé Borrion:** Conceptualization, Formal analysis, Writing – review & editing, Visualization, Validation.

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.

Appendix A. Participating organisations

Case ID	Organisation alias	Industry; size; sector
1	LawEnfJ	Law enforcement; SME; Public
2	GovSecJN	Local government; LE; Public
3	GovSecJ	Local government; LE; Public
4		
5		
6		
7	EducInstF	Education; LE; Public
8	EducInstFB	Education; LE; Public
9	LawEnfM	Law enforcement; SME; Public
10		
11	GovSecA	Local government; LE; Public
12	LawEnfJU	Law enforcement; SME; Public
13	HealthSerJU	Health; LE; Public
14		
15	LawEnfF	Law enforcement; SME; Public
16	ITOrgA	IT; SME; Private
17	ConstrSupA	Construction; SME; Private
18	EducOrgA	Education; SME; Public
19	SecOrgM	IT; SME; Private
20	ITOrgJL	IT; SME; Private
21	CloudProvJL	IT; SME; Private
22	InfOrgJL	Infrastructure; SME; Private
23	ConstrSupJ	Construction; SME; Private
24	RelOrgJ	Religion; SME; Private
25	SportClubJ	Entertainment; LE; Private
26	UtilOrgD	Utilities; LE; Private
27	VirtOrgD	IT; SME; Private
28	CleanOrgD	Cleaning; SME; Private
29	EducOrgD	Education; SME; Public
30	SerOrgD	Waste; SME; Private
31	EducCompD	Education; SME; Public
32	PrimOrgD	Education; SME; Public
33	LogOrgD	Logistics; SME; Private
34	ITCompD	IT; SME; Private
35	LogWarJ	Logistics; LE; Private
36	TranspOrgJ	Transport; LE; Private
37	CharOrgJ	Charity; SME; Private
38	EducInstJ	Education; LE; Public
39	DigMedM	Digital retailer; SME; Private
40	PrivCoJL	Transport; LE; Private
41	FinOrgJL	Finance; SME; Private

Appendix B. Phase 3 data analysis

Phase 3 Themes and relevant Code IDs	Paid Ransom Victims: *No of instances (P*/S*)*	Not Paid Ransom Victims: *No of instances (P/S)*	Categories from Phase 3
1.Encrypted data not critical to business continuity	0	10 (1/9)	AI*
2.Encrypted data critical to business continuity	8 (6/2)	22 (2/20)	AI
3. No resources got encrypted, but data got stolen	0	1 (1/0)	AI
4. Resources got encrypted, and data got stolen	1 (1/0)	0	AI
5. Critical systems not disabled (servers not affected)	0	4 (1/3)	AI
6. Critical system disabled (servers affected)	1 (1/0)	7 (1/6)	AI
7.Effective backups	2 (0/2)	23 (15/8)	AI
8.Partial backups	0	6 (2/4)	AI
9.Ineffective backups	6 (6/0)	4 (1/3)	AI
10.Clear incident response strategy	1 (0/1)	13 (12/1)	AI
11.Poor incident response strategy	6 (6/0)	3 (1/2)	AI
12. Lack of incident response strategy	0	1 (0/1)	AI
13.Full visibility of affected data/systems	1 (0/1)	18 (15/3)	AI
14.Lack of visibility of affected data/systems	1 (1/0)	2 (1/1)	AI
15. Time to recover	4 (0/4)	12 (11/1)	AI
16. Time pressure to recover fast (public services)	0	3 (0/3)	AI
17.Time pressure to recover fast (private business-related)	3 (3/0)	8 (1/7)	AI
18.Time pressure from attackers	2 (2/0)	0	AI
19. Prior experience with ransomware attacks	2 (0/2)	1 (1/0)	AI
20.No prior experience with ransomware attacks	5 (0/5)	2 (0/2)	AI
21. Decryption key available	0	1 (1/0)	AI
22. Data not fully digitised	0	4 (4/0)	AI
23. Recovery via collaboration	0	2 (2/0)	AI
24. No guarantee decryption key will be released	0	2 (0/2)	AI
25. Business loan not feasible	0	1 (0/1)	AI
26. Possibility of being asked for second ransom	0	2 (1/1)	AI
27.IT expert advice: "I know this gang – they have good reputation"	1 (1/0)	0	AI
28. IT expert advice: "Ransomware offenders normally release DK as they care about their reputation"	1 (1/0)	0	AI
29. Inadequate advice from authorities (ransom too large)	0	1 (1/0)	AI
30.Irreversable loss of important data (scientific=1; criminal=2)	3 (3/0)	4 (3/1)	PE*
31. Main business function not affected – business will continue without encrypted assets	0	12 (12/0)	PE
32. No loss of business continuity expected although important function affected	0	1 (1/0)	PE
33.Minor loss of business continuity expected	1 (0/1)	5 (5/0)	PE
34. Some loss of business continuity expected, affecting local community/staff/public/one business function	1 (0/1)	9 (2/7)	PE
35.Prolonged business continuity losses expected, affecting local community/staff	1 (0/1)	1 (0/1)	PE
36.Without encrypted data business significant losses on a daily basis are expected	3 (3/0)	4 (1/3)	PE
37. Business continuity is not affected	0	1 (1/0)	PE
38. Bankruptcy not realistic outcome	4 (0/4)	9 (9/0)	PE
39. Bankruptcy realistic outcome	3 (3/0)	6 (1/5)	PE
40. Ransom amount	3 (1/2)	3 (1/2)	PCB*
41. Reluctant to facilitate crime	0	3 (0/3)	PCB
42. Manageable financial implications	0	3 (0/3)	PCB
43.Unmanageable financial implications	0	1 (1/0)	PCB
44. The price of losing data greater than paying ransom	6 (6/0)	3 (2/1)	PCB
45. The ransom amount greater than the price of losing data	0	3 (1/2)	PCB
46. Loss of business continuity of one non-vital function	0	9 (9/0)	PCB
47. Cannot afford ransom payment but still will survive (public organisation)	0	1 (1/0)	PCB
48. Cannot afford ransom payment and will not survive (private organisation)	0	1 (1/0)	PCB
49.External IT provider slip: "We will pay ransom"	1 (1/0)	0	PCB
50. Pointless to pay – customer loss and immediate pain inevitable	0	2 (2/0)	PCB
51.Successful negotiation to reduce ransom	1 (1/0)	0	PCB
52.Unsuccessful negotiation to reduce ransom	0	2 (2/0)	PCB
53.No opportunity to negotiate ransom amount	2 (0/2)	1 (1/0)	PCB
54. Intention and budget to renovate IT infrastructure	0	1 (1/0)	PCB
55. No impact on business operations, but potential impact on reputation through media exposure (public prosecution)	0	1 (0/1)	PCB
56. Business operations are impacted, potential impact on reputation through media exposure (public prosecution)	1 (1/0)	0	PCB
57. Fear of prosecution by Information Commissioner	1 (1/0)	0	PCB
58. Potential secondary crimes affecting customers	1 (0/1)	1 (0/1)	PCB
59. No recovery required	0	1 (1/0)	PCB
60. Recovery will be very hard but still possible	0	19 (19/0)	PCB
61. Recovery is not a problem	2 (0/2)	9 (9/0)	PCB
62. Exceptionally hard recovery predicted but there is no choice	0	1 (1/0)	PCB
63. Recovery is not possible without paying	6 (6/0)	2 (1/1)	PCB
64. Recovery will be mildly hard but still possible	0	1 (1/0)	PCB

P* = primary reason to (not) pay.
AI* = available information.
S* = secondary reason to (not) pay.
PE* = probabilities of events.
PCB* = potential costs benefits.

Appendix C. Information Containers – 'Did not Pay'

Case IDs: 26 $C_{not\ paid}$	*Information Container 15:* ***Ineffective backups and response strategy/Poor visibility of network/Bankruptcy is not realistic outcome/Unsuccessful negotiation/Hard recovery***. Victim's critical data and systems got locked up. The organisation decided to pay due to poor recovery strategies. However, the amount was too high, and the negotiation did not bring any success. Fortunately, bankruptcy is not a realistic outcome for this victim, and they managed to recover from partial backups. The recovery was very tough.
Case IDs: 33 $D_{not\ paid}$	*Information Container 16:* ***Ineffective backups and response strategy/Poor visibility of network/Losses are significant on a daily basis/Bankruptcy is realistic outcome***. Critical data and systems that prevented the organisation from continuing business operations got encrypted; losses were significant on a daily basis. The victim considered payment but at the same time was reluctant to pay criminals. As the CEO realised that their company is facing bankruptcy, they decided to pay. However, at that very time, the director found a company that guaranteed recovery from ransomware. The victim paid and received a decryption key. Upon investigation, police discovered that the very same day a payment was made to the bitcoin account provided by ransomware criminals. Law enforcement concluded that IT company had links with offenders.
Case IDs: 11 $E_{not\ paid}$	*Information Container 17:* ***Ineffective backups and response strategy/Poor visibility of network/Extremely high impact on business/Exceptionally hard recovery***. The victim only had partial backups and no incident response strategy, while critical data and systems were completely paralysed. The organisation considered payment and contacted law enforcement seeking for help. The response team assessed the situation and advised not to pay as the ransom amount would be too high. Upon questioning the victim, it was identified that the advice was incorrect. The interviewee expressed their regret at not investigating the payment options further. The recovery was extremely difficult and lengthy.

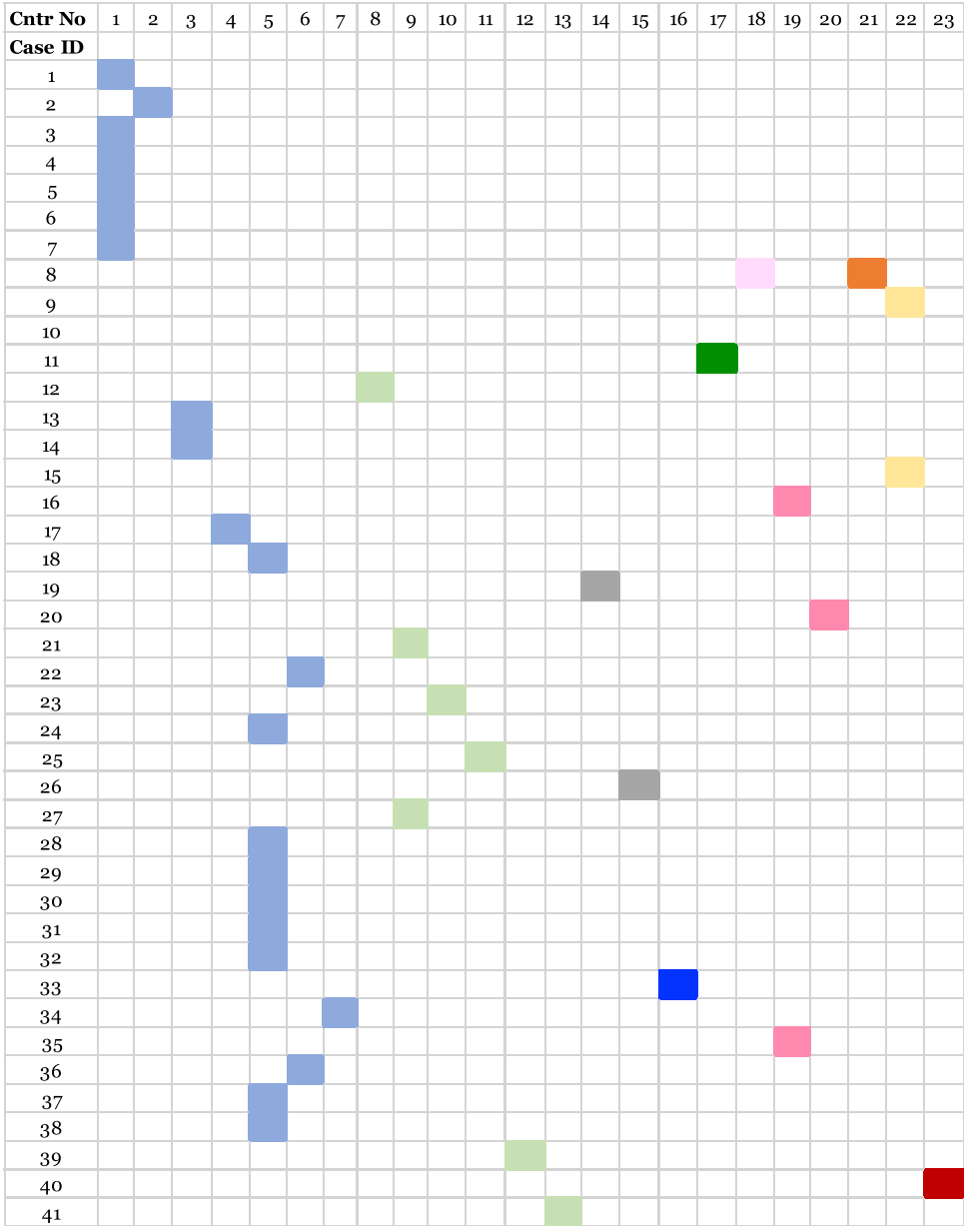
Appendix D. Information Containers – 'Paid'

Case IDs: 10 A_{paid}	*Information Container 18:* ***Effective backups and response strategy/Clear visibility of network/Feeling of responsibility***. The victim experienced a second ransomware attack two weeks after the first one. Although backups were available, IT service provider decided to pay ransom as they felt responsible for the second attack. With incremental backups, there is always a chance of some data loss (depends on how long ago backups were performed). The IT provider did not want the client to lose any data.
Case IDs: 16, 35 B_{paid}	*Information Container 19:* ***Ineffective backups and response strategy/Poor visibility of network/Bankruptcy is realistic outcome/Losses on a daily basis/Recovery would not be possible without data***. The victim experienced an unprecedented attack, where business losses were significant on a daily basis. Bankruptcy was a realistic outcome. The victim paid ransom.
Case IDs: 20 B_{paid}	*Information Container 20:* ***Ineffective backups and response strategy/Poor visibility of network/Bankruptcy is realistic outcome/Losses on a daily basis/Recovery would not be possible without data/Tough negotiation***. The victim experienced an unprecedented attack, where business losses were significant on a daily basis. The ransom was astronomically high, and the victim initiated very aggressive negotiation. Hackers reduced the amount, the organisation paid and received the key.
Case IDs: 8 C_{paid}	*Information Container 21:* ***Ineffective backups and response strategy/Poor visibility of network/Time pressure from attackers/Expert confirmation for payment/Irreversible loss of intellectual property/The price of losing data is higher than ransom/Recovery of data is not possible without paying***. The victim experienced an unprecedented attack where hundreds of devices got locked down. The main concern was the disappearance of intellectual property, although many critical systems were disabled too. This public organisation had been poorly prepared for the attack. Apart from poor backups, the organisation did not have a very clear visibility of the network, and therefore was not sure which data was gone. In the meantime, attackers gave the victim 72 h to pay. Therefore, the organisation could not even properly evaluate the situation. After inviting external experts to investigate the breach, it was agreed that the recovery of data was not possible without payment, and the decision was made to pay the attackers. Although bankruptcy was not a realistic scenario for this organisation, the effect of the attack could be too damaging for reputation within the international community.
Case IDs: 9, 15 D_{paid}	*Information Container 22:* ***Ineffective backups and response strategy/Poor visibility of network/Expert confirmation for payment/Irreversible loss of criminal data/The price of losing data is higher than ransom/Recovery of data is not possible without paying. S***The victims lost critical data, while no backups were available. The data was criminal evidence, which, if disappeared, could have detrimental consequences on the outcomes of criminal investigations, even setting some criminals free. No recovery was possible without a decryption key. Subsequently, the victim decided to pay. The fact that bankruptcy was not a realistic outcome was not relevant.
Case IDs 40 E_{paid}	*Information Container 23:* ***Fear of incrimination***. Criminals not only encrypted data, but also copied and transferred it to the attacker-controlled location. When the victim refused to pay, offenders threatened to report the breach to authorities. The victim paid due to fear of incrimination (both public by media and administrative by data protection officials).

Case IDs: 1, 3, 4, 5, 6, 7 $A_{not\ paid}$	*Information Container 1:* ***Effective backups and response strategy/Clear visibility of network/Minor impact on business operations/Straightforward recovery***. The victim emphasised that effective backups, clear incident response strategy, and full visibility of affected data/systems led to the swift recovery. Overall, the impact on business operations was minor.
Case IDs: 2 $A_{not\ paid}$	*Information Container 2:* ***Poor incident response strategy/High impact on business/Hard recovery***. The victim emphasised that although they had effective backups and full visibility of affected systems, the lack of incident response strategy delayed the response, allowing ransomware to spread to many systems, which gravely affected the services this organisation provides to the public. Although the recovery was predicted to be difficult, they still had an opportunity to regain control of their systems. It must be noted that this is a public organisation, and bankruptcy is not a realistic outcome.
Case IDs: 13 and 14 $A_{not\ paid}$	*Information Container 3:* ***Effective backups and response strategy/Clear visibility of network/Some loss of business continuity – too many machines affected/Hard recovery***. The victim demonstrated an exceptional level of preparedness for cyber breaches. However, this particular variant of ransomware (lateral movement functionality) spread on hundreds of devices, affecting critical data and, subsequently, certain business operations. The victim predicted tough recovery. The interviewee commented that if the servers were also affected, the outcome of this incident could be much more dramatic.
Case IDs: 17 $A_{not\ paid}$	*Information Container 4:* ***Ineffective backups and response strategy/Poor visibility of network/The type of data affected/Not fully digitised/Hard recovery***. Although the victim was poorly prepared for a ransomware attack, they were somewhat fortunate that the encrypted data was not immediately needed to continue business operations. Therefore, the organisation had time to recover. Furthermore, the victim has not fully migrated to the digital mode and had printed copies of some data. The organisation recovered data via printed copies of documents. Still though the victim found recovery very challenging.
Case IDs: 18, 24, 28, 29, 30, 31, 32, 37, 38 $A_{not\ paid}$	*Information Container 5:* ***Data encrypted not critical to business continuity/Easy recovery***. The victim could continue business-as-usual because the data affected was not critical to business continuity. One victim in this category had poor recovery strategies, and yet found recovery relatively easy.
Case IDs: 22, 36 $A_{not\ paid}$	*Information Container 6:* ***Effective backups and response strategy/Clear visibility of network/Some loss of business continuity expected/Bankruptcy is not realistic outcome/Hard recovery***. Although both critical data and systems got encrypted, and the breach affected business continuity, the organisation had effective recovery measures in place. This company provides a critical infrastructure to the government; therefore, bankruptcy is not a realistic outcome for this organisation. However, this particular ransomware variant has advanced propagation abilities, and spread to hundreds of devices. Therefore, the recovery was challenging.
Case IDs: 34 $A_{not\ paid}$	*Information Container 7:* ***Effective backups and response strategy/Clear visibility of network/Some loss of business continuity expected/Hard recovery***. Although both critical data and systems got encrypted, and the breach affected business continuity, the organisation had effective recovery measures in place. Though recovery was still predicted to be hard.
Case IDs: 12 $B_{not\ paid}$	*Information Container 8:* ***Ineffective backups and response strategy/Poor visibility of network/Decryption key/Easy recovery***. Although this breach could potentially have had dramatic consequences, the victim contacted external a cyber response team that managed to discover a decryption key for this particular ransomware variant.
Case IDs: 21, 27 $B_{not\ paid}$	*Information Container 9:* ***Effective backups and response strategy/Clear visibility of network/Pointless to pay – customer loss and immediate pain are inevitable/Hard recovery***. Critical data that prevented the organisation from continuing business operations got encrypted; losses were significant on a daily basis. The victim considered payment but realised that decryption key will not speed up their recovery. Since the organisation was well prepared for cyberattacks, they made a decision to recover from backups.
Case IDs: 23 $B_{not\ paid}$	*Information Container 10:* ***Ineffective backups and response strategy/Poor visibility of network/Time to recover/Recovery via collaboration/Business can continue for a while/Hard recovery***. This organisation was poorly prepared for the ransomware attack. But, fortunately, immediate business continuity did not depend on this data. Therefore, some time was available for recovery. The victim recovered via collaboration. The recovery was very difficult.
Case IDs: 25 $B_{not\ paid}$	*Information Container 11:* ***Partial backups/Clear visibility of network /Time to recover/Data not fully digitised/Hard recovery***. This organisation was very fortunate as the data that got encrypted was generally critical to business but was required to be used in a few days after the attack. Therefore, they had time. The victim considered payment, but the ransom was too high. After realising that some of lost data was available as printed copies, they decided to recovery without paying the ransom. The victim expected very tough recovery.
Case IDs: 39 $B_{not\ paid}$	*Information Container 12:* ***Ineffective backups and response strategy/Poor visibility of network/Fear to be asked for second ransom/Bankruptcy is realistic outcome***. This breach could potentially cost the victim its business. However, the ransom was very high, and negotiation to reduce the amount was unsuccessful. Besides, the victim was afraid that even if they pay, the criminals will ask for a second ransom (perceived as an 'easy target'). In that case, the company would definitely be liquidated. The organisation decided to attempt to recover from partial backups. Recovery was incredibly hard but successful.
Case IDs: 41 $B_{not\ paid}$	*Information Container 13:* ***Effective backups and response strategy/Clear visibility of network/Some loss of business continuity expected/Bankruptcy is not realistic outcome/Hard recovery***. Although no resources got encrypted, hackers stole very sensitive data (customer data was copied and transferred to the attacker-controlled location). Nevertheless, the organisation could continue 'business-as-usual'. Although the company had effective recovery measures in place, it did not play any role in this particular attack. Because hackers had the actual copy of data, the victim was afraid to become a target of indefinite blackmail. Besides, the director had a strong belief that it is wrong to facilitate crime. Although the company was aware of possible public prosecution, they have chosen to take risk and inform customers of the breach.
Case IDs: 19 $C_{not\ paid}$	*Information Container 14:* ***Ineffective backups and response strategy/Poor visibility of network/Could not afford ransom payment/Negotiation impossible – bankruptcy***. The victim experienced unprecedented attack where critical data and systems were locked down, so the business could not continue their operations. The organisation wanted to pay, but they could not afford the ransom payment. The victim wanted to initiate negotiation, but hackers did not leave any contact information. As a result, the organisation closed down their operations.

(*continued on next page*)

Appendix E. Phase 5 data analysis



Colour codes 'did not pay':

Light blue – 'had not intention to pay'

Light green – 'considered payment'

Grey – 'wanted to pay but could not afford to'

Blue – 'shabby IT provider'

Green – 'regretful decision'

Colour codes 'paid':

Pink – 'IT provider feeling responsibility'

Bright pink – 'threat of bankruptcy'

Orange – 'intellectual property loss'

Yellow – 'criminal data loss'

Red – 'fear of incrimination'

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. Comput. Secur. 74, 144–166.

Bisson, D. (2020) Increase in ransomware demand amounts driven by Ryuk, Sodinokibi, *Trip Wire*, 4 May, available at: https://tinyurl.com/2rujqpjd [Accessed 20th September 2020].

Boss, S.R., Kirsch, L., Angermeier, I., Shingler, R., Boss, R., 2009. If someone is watching, I will do what I am asked: mandatoriness, control, and information security. Eur.J. Inf. Syst. 18 (2), 151–164.

Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.

Cacciotti, G., Hayton, J.C., 2015. Fear and entrepreneurship: a review and research agenda. Int. J. Manag. Rev. 17, 165–190.

Cartwright, E., Hernandez Castro, H., Cartwright, A., 2019. To pay or not: game theoretical models of Ransomware. J. Cybersecur. 5 (1), 1–12.

Chen, M.F., 2016. Impact of fear appeals on pro-environmental behavior and crucial determinants. Int. J. Advert. 35 (1), 74–92.

College of Policing [CoP] (2016) Competency and values framework for policing, Report, *CoP*, available at: https://d17wy4t6ps30xx.cloudfront.net/production/uploads/2017/09/Competency-and-Values-Framework-for-Policing_4.11.16.pdf [Accessed May 2021].

Connolly, L., Wall, D., 2019. The rise of crypto-Ransomware in a changing cybercrime landscape: taxonomising Countermeasures. Comput. Secur. (87) 1–18.

Connolly, L., Borrion, H., 2020. Your money or your business: decision-making processes in ransomware attacks. International Conference on Information Systems (ICIS 2020).

Connolly, L., Wall, D., Lang, M., 2020. An Empirical investigation of ransomware attacks on organisations: an assessment of severity and salient factors affecting vulnerability. J. Cybersecur. 6 (1), 1–18.

Connolly, L., Lang, M., Taylor, P. and Corner, P. (2021) The evolving threat of ransomware: from extortion to blackmail, *available online:* https://www.preprints.org/user/home/submissions (preprint).

Dodd, V. (2020) Police in England and Wales facing 'new era of austerity', The Guardian, 1 July, available at: https://www.theguardian.com/uk-news/2020/jul/01/police-warn-of-cuts-to-funding-even-worse-than-in-austerity-years [Accessed March 2021].

Europol (2020a) Internet Organised crime threat assessment 2019, Report, *Europol*, available at: Users/lena/Downloads/internet_organised_crime_threat_assessment_iocta_2020.pdf [Accessed: 11th December 2020].

Europol, 2020b. How is Ransomware different during the COVID-19 pandemic? Europol. available at https://www.europol.europa.eu/covid-19/covid-19-ransomware. [Accessed May 2020].

Eaton, C., Volz, D., 2020. Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom. Wall Street J.. 19 May, available at https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636 . [Accessed June 2021].

Ferguson, S. (2019a) Florida city paying $600,000 to end ransomware attack, Bank Info Security, 20 June, available at: https://www.govinfosecurity.com/florida-city-paying-600000-to-end-ransomware-attack-a-12673 [Accessed September 2020].

Ferguson, S. (2019b) Georgia County pays $400,000 to Ransomware attackers, Bank Info Security, 12 March, available at: https://www.bankinfosecurity.com/georgia-county-pays-400000-to-ransomware-attackers-a-12159 [Accessed September 2020].

Furber, C., 2010. Framework analysis: a method for analysing qualitative data. Afr. J. Midwifery Women Health 4 (2), 97–100.

Hazam, S., Felsenstein, D., 2006. Terror, fear and behaviour in the Jerusalem housing market. Urban Stud. 44 (13), 1529–1546.

Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services [HMICFRS] (2019) Cyber: keep the light on, Report, *HMICFRS*, available at: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/cyber-keep-the-light-on-an-inspection-of-the-police-response-to-cyber-dependent-crime.pdf [Accessed April 2021].

Huang, D.Y., Aliapoulios, M.M., Li, V.G., Invernizzi, L., McRoberts, K., Bursztein, E., Levin, J., Levchenko, K., Snoeren, A.C., 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 Sci. 8 (2), 1–22.

Interpol (2020) Cybercriminals targeting critical healthcare institutions with Ransomware, *Interpol*, 4 April, available at: https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware [Accessed May 2020].

Johnson, A.C., Warkentin, M., 2010. Fear appeals and information security behaviors: an empirical study. MIS Q. 34 (3), 549–566.

Mansfield-Devine, 2018. The malware arms race. Comput. Fraud Secur. 2018 (2), 15–20.

Miller, J. (2020) What is network visibility and how do you maintain it?*BitLyft*, 10 December, available at: https://www.bitlyft.com/what-is-network-visibility-how-do-you-maintain-it [Accessed April 2021].

Morgan, S., 2020. Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine. 13 November, available at https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021. [Accessed December 2020].

National Cyber Security Centre [NCSC] (2020) Advisory: COVID-19 exploited by malicious cyber actors, *NCSC*, 8 April, available at: https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory [Accessed May 2020].

Ndichu, D. (2021) Kaspersky: over half of ransomware victims paid off attackers in 2020, Kaspersky, 4 April, available at: https://gulfbusiness.com/kaspersky-over-half-of-ransomware-victims-paid-off-attackers-in-2020/#:~:text=More%20than%20half%20(52%20per,stolen%20data%2C%20the%20report%20adds [Accessed May 2021].

O'Donnell, L. (2020) University of Utah pays $457K after Ransomware attack, Threat Post, 21 August, available at: https://threatpost.com/university-of-utah-pays-457k-after-ransomware-attack/158564 [Accessed March 2021].

Papp, J., Smith, B., Wareham, J., Wu, Y., 2019. Fear of retaliation and citizen willingness to cooperate with police. Polic. Soc. 29 (6), 623–639.

Ritchie, J., Spencer, L., 1994. Qualitative data analysis for applied policy research. In: Bryman, A., Burgess, R.G. (Eds.), Analyzing Qualitative Data. NY: Routledge, New York, pp. 173–194.

Simmonds, M., 2017. How businesses can navigate the growing tide of ransomware attacks. Comput. Fraud Secur. (3) 9–12.

Tidy J. (2020) How hackers extorted $1.14m from University of California, San Francisco, *BBC*, 29 June, available at: https://www.bbc.com/news/technology-53214783 [Accessed April 2020].

Virgo, P. (2021) Making sense of the changing UK cyber policing and skills scene, *Computer Weekly*, 4 March, available at: https://www.computerweekly.com/blog/When-IT-Meets-Politics/Making-sense-of-the-changing-UK-Cyber-Policing-and-Skills-Scene [Accessed March 2021].

University of California San Francisco [UCSF] 2021. UC part of nationwide cyber attack, *UCSF*, 31 March, available at: https://ucnet.universityofcalifornia.edu/news/2021/03/uc-part-of-nationwide-cyber-attack.html [Accessed May 2021].

University of Stanford [UoS] 2021. Statement on the School of Medicine cybersecurity incident, *UoS*, 2 April, available at: https://med.stanford.edu/connected/announcements/cybersecurity-incident-2021.html [Accessed May 2021].

University of California Berkeley [UCB] 2021. UC email security incident, UCB, 31 March, available at: https://technology.berkeley.edu/news/uc-email-security-incident [Accessed May 2021].

Zhao, J.Y., Kessler, E.G., Yu, J., 2018. Impact of trauma hospital ransomware attack on surgical residency training. J. Surg. Res. 232, 389–397.

Zhang-Kennedy, L., Assal, H., Rocheleau, J., et al., 2018. The aftermath of a cryptoransomware attack at a large academic institution. In: Proceedings of the 27th USENIX Security Symposium. Baltimore, MD, pp. 1061–1078 15–17 August 2018ISBN 978-1-939133-04-5.

Dr Alena Y Connolly (PhD) is an Assistant Professor at Zayed University. She has conducted her PhD at the National University of Ireland Galway and University of California Berkeley. Her research interests include cybercrime, human factors in security, ransomware and security countermeasures in organisational settings. Before joining Zayed University, she worked at several UK and Irish universities, including University College London, University of Leeds, National University of Ireland Galway and University of Bradford. She is a winner of a Fulbright Scholarship.

Dr Hervé Borrion (PhD) is Deputy Head of Department at the UCL Department of Security and Crime Science. He pursued his postgraduate education at the Ecole Nationale Supérieure d'Aéronautique et de l'Espace in France and at University College London. He contributes his expertise in systems modelling to better understand and address crime problems ranging from poaching to terrorism through cybercrime. A strong advocate of problem-orientated and engineering methodologies, he has held advisory positions on various committees including the EU Centre for National Infrastructure Protection, MoRiLE harm matrix project, UK Council for Graduate Education and the Open University Policing Centre. Currently, he devotes most of his research time to support the National Police of Colombia during the COVID-19 crisis.