*"*There was a bit of PTSD every time I walked through the office door*":* Ransomware harms and the factors that influence the victim organisation's experience

Gareth Mott, School of Politics and International Relations and Institute of Cyber Security for Society, University of Kent, Canterbury, CT2 7NZ, UK

Sarah Turner, School of Computing and Institute of Cyber Security for Society, University of Kent, Canterbury, CT2 7NZ, UK

Jason R.C. Nurse*, School of Computing and Institute of Cyber Security for Society, University of Kent, Canterbury, CT2 7NZ, UK

Nandita Pattnaik, School of Computing and Institute of Cyber Security for Society, University of Kent, Canterbury, CT2 7NZ, UK

Jamie MacColl, Royal United Services Institute (RUSI), London, SW1A 2ET, UK

Pia Huesch, Royal United Services Institute (RUSI), London, SW1A 2ET, UK

James Sullivan, Royal United Services Institute (RUSI), London, SW1A 2ET, UK

*Corresponding author:
Jason R.C. Nurse, School of Computing and Institute of Cyber Security for Society, University of Kent, Canterbury, CT2 7NZ, UK
j.r.c.nurse@kent.ac.uk
+44 (0)1227 82 7134

Abstract

Ransomware is a pernicious contemporary cyber threat for organisations, with ransomware operators intentionally leveraging a range of harms against their victims in order to solicit increasingly significant ransom payments. This article advances current research by engaging in a topical analysis into the depth and breadth of harms experienced by victim organisations and their members of staff. We therefore enhance the understanding of the negative experiences from ransomware attacks, particularly looking beyond the financial impact which dominates current narratives. Having conducted an interview or workshop with 83 professionals including ransomware victims, incident responders, ransom negotiators, law enforcement and government, we identify a wide array of severe harms. For organisations, the risk of business interruption and/or data exposure presents potentially highly impactful financial and reputational harm(s). The victim organisation's staff can also experience a range of under-reported harms, which include physiological and physical harms that may be acute. We also identify factors that can either alleviate or aggravate the experiencing of harms at organisational and employee level; including ransomware preparedness, leadership culture and crisis communication. Given the scale and scope of the identified harms, the paper provides significant new empirical evidence to emphasise ransomware's positioning as a whole-of-organisation crisis phenomenon, as opposed to an 'IT problem'. We argue that the wider discourse surrounding ransomware harms and impacts should be reflective of the nature of the real-term experience(s) of victims. This, in turn, could help guide efforts to alleviate ransomware harms, through improved organisational ransomware preparedness and tailored post-ransomware mitigation.

Keywords: cyber security, ransomware, harms, victim experience, malware, human aspects, psychological harm, financial harm, cyberpsychology, cybercrime.

Introduction

Ransomware has come to be regarded as a particularly insidious form of malicious cyber activity. Contemporary ransomware intentionally seeks to leverage two critically impactful risks organisations fear; sustained business interruption and targeted or mass data leakage [1]. Although ransomware's impacts are global, the challenge is particularly endemic for organisations in the most-targeted states, with the USA, the UK and Canada comprising the top-three targeted jurisdictions [2]. With many ransomware operators situated in nation-states with whom Western relations are relatively poor – notably the Russian Federation – ransomware merges professionalised cybercrime with intractable geopolitics [3]. It is in this context that the UK government recently categorised ransomware as the "most significant cyber threat facing the UK" in the revised *National Cyber Security Strategy* [4].

Concerningly, ransomware has impacted critical national infrastructure providers in the UK, including NHS Trusts [5], Hackney and Redcar Councils [6, 7] and Staffordshire Water [8]. In the USA, a 2021 ransomware attack against Colonial Pipeline impacted the supply of petroleum products [9]. A 2022 ransomware attack in Costa Rica had protracted impacts for wide-ranging government services, including the halting of imports and exports due to system unavailability [10]. In this light, ransomware is demonstrably, not a hypothetical risk; nor is it an 'IT problem'. Ransomware is both an acute risk for contemporary organisations and additionally represents a national and/or societal security threat.

While the significance of ransomware attacks is generally acknowledged, their exact effects and the scale and harms (e.g., negative physical, economic, and societal impacts) at an organisational and individual level vary. Without a better understanding of the harms created by ransomware, researchers, policymakers and practitioners risk misunderstanding the impact ransomware has on society and its citizens. Designing effective responses to the challenges presented by ransomware – particularly around the underreporting of ransomware and victims' willingness to pay ransoms – requires insight into the impact ransomware has on organisations, their employees, and their wider third parties, including their business partners and clients, and the wider society.

We aim to address this gap in knowledge by conducting research into the harms caused by ransomware attacks, the experiences of victims who have been affected, and key factors influencing those experiences. Our study is scoped to the direct victims of ransomware attacks, specifically the directly-targeted organisations and their employees. We define 'victim experience' as the impressions that a ransomware victim notices or feels during and after an incident. Ultimately, our work seeks to answer the question: What harms do victims of ransomware experience and what factors alleviate or aggravate those harms? We approach this research question through an exploratory research approach. Harms and the experiencing of harm(s) are both objective and subjective; throughout our research, interviewees have been empowered to define and convey their own experiences. Focusing in the objective need to fill the research gap in understanding the 'lived' impacts of ransomware, we analyse these vernacular expressions of the ransomware victim experience.

This article provides evidence-based insights into a victim's experience of ransomware harms at a critical conjuncture of the evolution of the threat, amidst a period of acute policymaking and organisational interest [11, 12]. Identifying the breadth and depth of ransomware harms against organisations and their employees – and factors that can alleviate or exacerbate these harms – can assist in the ongoing practitioner and research endeavour to improve resiliency against ransomware. Furthermore, given that organisations may resort to paying a demanded or negotiated ransomware payment reluctantly and in-extremis, identifying ways in which harms can be alleviated may offer insights into steps that an organisation can take before and during an incident that would reduce their propensity to pay. At a policy level, this research befits a government's approach to cyber security, wherein prevention is supplemented by 'resiliency' [13, 14]; in essence, the ability to 'bounce back' in

the aftermath of an incident. In the absence of a 'silver bullet' solution for the ransomware scourge [15], incremental measures to alleviate ransomware harms can be part of a broader package of solutions to improve organisational resiliency and reduce the success-rate of the business model(s) of ransomware operators.

Drawing on a large qualitative data corpus comprising 83 unique interview and workshop participants predominantly based in the UK (with a small number also based in Western Europe, the USA and internationally), we identify a range of pertinent findings at a critical conjuncture in the marked growth of ransomware as an organisational and societal issue. This article finds that ransomware is an acute business risk for contemporary organisations, particularly given its capacity to cause sustained business interruption within a relatively short space of time. A core underpinning narrative that victims – and those who support victims – identified was that a ransomware incident is not an 'IT problem', but is instead a whole-of-organisation crisis.

Aligning with existing reporting [16], organisational harms were most-prominently categorizable as either 'financial' or 'reputational' harms. However, the study also identified a range of potentially significant harms that may be suffered by IT and non-IT staff an organisation suffering a ransomware breach. Whilst some of these harms may correlate with the harms experienced by the organisation, there are also divergences. Of particular note was the presence of potentially severe physiological and psychological harm that may arise from the fallout and handling of the incident. These harms are significant for the employees at victim organisations, but are often under-reported in wider ransomware-impact discourse. Importantly, our research also identifies a range of factors that can serve to either alleviate or exacerbate the breadth and depth of harms. Factors over which the victim organisation is likely to have a degree of control include preparedness, leadership culture, and crisis communication. Through a heightened understanding of the breadth and depth of harms at organisational and staff level – as well as factors that influence these harms – organisations may be better-placed to effectively manage a ransomware incident.

The ensuing article is structured in five sections. Firstly, we summarise existing literature to understand the experiences of victims of ransomware attacks, including a reflection on the methods through which such insights have been gathered. Secondly, the article outlines the qualitative methodological approach underpinning our research. The results of the interviews and workshops are presented next, which establishes the basis for the following section: a discussion of the core themes arising from the presented data. Lastly, a conclusion summarises the main contributions of the research, and outlines scope for further work.

Literature review

The financial cost of ransomware attacks

In order to assess the scale and scope of ransomware harms, it is necessary to map them through research. Aggregated quantitative data has indicated marked growth in the scale and scope of ransomware [17, 18]. There has been growth in the cadence of attacks, the breadth of ransomware strains, and the value of demanded/negotiated ransoms [19]. It has been reported that in 2020, there were 304 million ransomware attacks globally [20]. The UK's Information Commissioner's Office (ICO) has published data highlighting a doubling of reported ransomware attacks from 2020 to 2021 [21]. A Sophos [22] report drawing on survey data from organisations in 31 different nation-states indicated that the average ransom paid by mid-sized organisations was $812,360 and that the average cost of

repair, business interruption, lost opportunity, and ransom (if paid) was $1.4 million[1]. The 2023 Sophos report [23] identified that the average ransom payment had increased to over $1.5 million and that recovery costs had increased to $1.85 million[2]. The 2024 DSIT Cyber Breaches Survey also provides insights into the financial impact of ransomware – and other cyber breach – events. The Survey involved randomised surveys of 2,000 businesses, 1,004 charities and 430 education institutions, in addition to 44 in-depth qualitative interviews [68]. These impacts included: additional staff time to handle a breach; costs of new measures to prevent future incidents; loss of productivity; loss of intellectual property; and cost of equipment replacement. This reflects not only the lost opportunity and remediation cost(s) of the initial breach itself, but also the material feed-forward costs of future breach prevention.

Such overt and costly downtime is likely to have direct and downstream impacts. These impacts would, feasibly, be experienced by the impacted organisation, their staff, their business partners, their clients and potentially wider third parties. However, whilst monetary cost is an objective way to estimate the degree of harm experienced by organisations and individuals, there are protracted and significant challenges in assessing the bona fide financial cost of ransomware, as highlighted in a CISA review [24]. Additionally, a focus on financial costs may be blinkered, as this could overlook non-financial harms, such as the psychological impacts that victims may experience during and after a ransomware incident. Given the prominence of ransomware impacts, existing research has sought to provide insights through victim interviews/surveys, expert interviews/surveys, case studies and broad surveys.

The harms experienced after ransomware attacks: Existing approaches

Interviews with victims provide an opportunity for researchers to gain a significantly greater depth of knowledge of the ransomware 'victim experience' than may otherwise be gleaned through a simple survey or publicly-accessible news reports. One example of such research is that produced by Connolly et al. [25], in which the authors conducted semi-structured interviews with IT and security managers from ten organisations based either in the UK or USA that had been victim to ransomware attacks. These interviews sought to form an understanding of the severity and characteristics of the respective attacks. The interview responses were then juxtaposed with case studies drawing on a broader set of ransomware attacks to understand the role that an organisation's characteristics may play in the outcomes of a ransomware attack. Connolly et al.'s study [25] identified that whilst organisation size had little impact on the severity of a given ransomware incident (including recovery time), the organisation's sector did; accordingly, private organisations were more severely affected than public sector organisations. The authors suggested that this was – potentially – due to the nature of public sector organisations as 'sole suppliers' that are 'publicly funded'. In essence, the sole-provider nature of these organisations meant that they were not subject to the loss of trade or clients that private sector organisations are more likely to be subjected to. Of note, however, with respect to Connolly et al.'s study [25] is the relative absence of consideration of the broader impacts of loss of essential services to the public.

Another relevant study is that produced by the UK's Department for Digital, Culture, Media and Sport (DCMS) [26], in which researchers conducted interviews with ten victim organisations (two employees per organisation) to create case studies. These organisations ranged in terms of size and sector. The

[1] Respondents to the 2022 Sophos report were from: Australia, Belgium, Brazil, Canada, Chile, Colombia, Czech Republic, France, Germany, Hungary, India, Israel, Italy, Japan, Malaysia, Mexico, Netherlands, Nigeria, Philippines, Poland, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, UAE, UK and the USA.

[2] Respondents to the 2023 Sophos report were from: Australia, Austria, Brazil, France, Germany, India, Italy, Japan, Singapore, South Africa, Spain, Switzerland, UK and USA.

report drew upon the interview data to build case studies of each organisation's cyber-breach experience, with interviews substantively informing: the organisations' background, their cybersecurity levels pre-breach, their response to the breach, and the impacts that the breach had on the organisation. The DCMS study identified significant distinctions in the victim experience, which differed on the basis of organisation size, attack scale, IT usage, and security response. A separate DCMS-supported study argued for a toolkit for assessing the cost(s) of ransomware attacks against organisations; noting that in some cases, re-assessment of the cost of a given incident markedly increased [27]. For instance, in one example, after using the toolkit, an IT director at a large organisation raised their estimated costs of a ransomware incident that they had suffered from £200,000 to £300,000 [27].

Whilst the above studies draw on a range of victim organisations to build a corpus of data highlighting areas of similarity and divergence between differing cases, other studies have instead focused on a singular incident. For instance, a research study by Zhang-Kennedy et al. [28] focused on a specific ransomware attack against a large US university in 2016. Instead of focusing on the victim experience from the standpoint of managers and IT professionals, the authors examined the experience of students, faculty and staff, drawing on a survey of 150 participants and interviews with a further 30 of those affected by the attack. Additionally, the research investigated the victim experience of individuals and their perspective of the incident, including their emotional reactions. Participants were also asked about their security practices before and after the incident. The authors supplemented the surveys with interviews, allowing for a more in-depth exploration of the impacts and emotions that individuals experienced. One finding was that there was a perceptible negative impact on the victims' emotional states, including elevated frustration, anger and concern; feelings that were exacerbated by the perceived lack of communication from the university during the incident. Negative emotional impacts were exhibited by victims who did not themselves experience data loss [28].

Other studies focusing on singular ransomware incidents include investigations of ransomware attacks against healthcare organisations in Ireland and the USA, respectively [29, 30]. In both of these studies, the authors engaged with impacted staff rather than specifically IT professionals; i.e., interviewees included trainee doctors, surgeons and other clinicians. Whilst the study did not identify disruption to clinical outcomes, interviewees nonetheless highlighted how the incidents affected their duties. Zhao et al. [30] also asked participants about the emotional toll that they had experienced. A particular finding was that colleagues involved in trauma patient care experienced increased levels of stress as a result of the loss of critical systems during the ransomware attack. Collectively, these research studies focusing on interviewing stakeholders involved in singular ransomware incidents highlight a core utility of in-depth interviews; the victims are able to convey their experiences in a full-form and nuanced way. This, in turn, enables the researcher to gain a fuller understanding of the depth and breadth of ransomware harms. However, at the same time, as the researchers acknowledge [30], the focus on a singular incident is a limitation. We propose that there are significant benefits to be gained from engaging with stakeholders across multiple ransomware incidents. This would increase the depth and breadth of the subsequent results. It would also enable a space for a within-study comparison of the 'victim experience' across differing ransomware incidents.

Whilst contemporary ransomware activity is often attributed to increasingly professionalised targeting of organisations and/or access brokering [31], comparatively automated ransomware against micro-Small-to-Medium-sized Enterprises (SMEs) and individuals continues [32]. Some research has been conducted with respect to attacked home-users; for instance, Simiou et al.'s [33] survey of 1,180 US residents and Ortloff et al.'s [34] survey of 963 German residents. Respondents were asked to self-report whether they had been a victim of a ransomware incident. Drawing on the descriptions of the purported incidents, the authors filtered the responses and conservatively estimated that 6% (US) and 8.3% (German) of respondents were victims of ransomware [33, 34].

Another study, authored by Button et al. [35], drew on interviews with 38 home users and 14 employees from UK SMEs who were victims of computer misuse crimes (seven of which were ransomware victims). The study did not draw a distinction between the home and SME victims. Button et al. [35] examined the interview corpus to identify the victim experience of the individuals, pinpointing a range of harms, including damage to physical property, psychological and emotional impact and financial loss.

Broad surveys can be used to gain insight into ransomware victim experiences [36, 37, 38, 39]. For instance, researchers can use surveys – which include non-victim participants – to gauge general perspectives about ransomware risks and impacts. Haner et al. [40] surveyed 1,013 US residents to gauge their feelings about a range of ransomware scenarios. Separately, a study by Mujaye [37] surveyed 27 IT professionals from a range of nation-states (including the USA, Netherlands and South Africa), asking respondents about whether a ransom payment should be paid by a given organisation. The study identified that only 4% of participants advocated ransom payment, with 48% being equivocal [37]. Whilst these studies examined hypothetical scenarios, this broad survey approach has also been applied to ransomware case studies. For instance, research by Shandler and Gomez [41] surveyed 707 residents of North Rhine-Westphalia a week after a ransomware attack against Düsseldorf University Hospital. Participants were asked about their confidence in the German government's management of cyber security and the emotions that they experienced after the attack. Shandler and Gomez [41] suggested that ransomware attacks had the potential to undermine social cohesion, with the residents reporting a decrease in their trust in the government following the hospital incident.

Understandably, the recruitment of ransomware victim interviewees can be challenging. Nonetheless, one approach that existing studies have taken to mitigate interviewee-recruitment challenges is to draw on reports and publicly-available data relating to ransomware events in order to infer findings about the victim experience. These studies typically focus on a single ransomware incident. For instance, Caroscio et al. [42] focus on two Babuk attacks perpetrated against the Washington DC Metropolitan Police Department and an aerospace contractor, respectively. The authors outline the timelines and modalities of the attacks and subsequently conduct a high-level analysis of the impacts. Separately, Jarjoui et al. [43] focus on a ransomware attack against an Australian alcoholic beverage manufacturer. In a similar fashion to Caroscio et al. [42], the authors present a timeline of the attack, before discussing the operational and economic impacts [43]. A recent study by Pattnaik et al. [44] drew on public sourcing of eight ransomware cases from 2017 to 2021 to model a range of financial and non-financial harms, identifying prominent social and human harms present across differing victim-sectors. Such studies offer valuable insight into victims' experiences of ransomware harms by drawing on secondary data. The capacity to develop comparison studies [44] is also insightful for identifying areas of divergence and convergence between ransomware harms and the victim experience. However, there are potential limitations to the nuance and detail that can be gleaned from secondary data such as news reporting and public reports.

Understanding the ransomware harms and the victim experience: research gaps

The above exploration of the state-of-the-art in the victim experience of ransomware harms and ransomware incident management suggests pressing research gaps. Given the challenges of accessing ransomware victim participants, there is a need for further research drawing on multiple participants. Furthermore, limited pools of interviewees and incidents reduce the scope for researchers to make assessments of the timeline of experienced ransomware harms; particularly mid or long-term harms. There is also a tendency to analyse the victim experience of ransomware from either an organisational

or an individual basis; whereas pertinent findings may be found in the synergy and contention between the two. Finally, whilst – commendably – there is existing research that considers the non-financial harms of ransomware, such as its psychological effects on direct or indirect parties, further research is warranted in this area, particularly drawing on interviewees who experienced attacks that occurred across 2020, 2021 and 2022, given the recent escalation in the reported financial harms [22, 23].

Importantly, a stronger empirical understanding of the financial and non-financial harms that victims experience during and after a ransomware event can: (i) better inform organisations about the possible impacts that they and their staff may experience; (ii) assist them in preparing mitigation strategies to alleviate impacts; and (iii) better inform wider society about the overall impact(s) that ransomware causes against victims. In essence, the ongoing effort to improve our understanding of ransomware harms is an important and necessary step to increase empathy, increase resiliency, and inform policymaking decisions that may have an influence on ransomware victims.

These aforementioned research gaps compose the area where our research sits. As highlighted in the study-rationale included in the introductory section of this paper, we approach this research in an exploratory manner. This approach empowers ransomware victims – and those who work alongside substantial numbers of ransomware victims – to express ransomware harms and the ransomware victim experience in their own words. Importantly, this research contributes to gaps in the field of literature in a number of ways. Firstly, we have held long-form interviews with a comparatively large number of ransomware victims and the ransomware support ecosystem. Secondly, the ransomware victims represent diverse sectors, intra-organisational roles and organisational size. Thirdly, given the dynamic nature of the ransomware threat, our data corpus captures the victim experience in the midst of a distinct evolution in ransomware groups' tactics. Chiefly, this is the growing prominence of data exfiltration as a form of extortion leverage. These three points also consequently highlight primary areas of novelty.

We draw on our data corpus to develop an analysis of the scope and scale of ransomware harms. To synthesise findings, we also include two comprehensive tables that capture all of the harms that were identified by interviewees and workshop participants. The first table focuses on 'organisational'-level harms, and the second table focuses on harms-to-staff within those organisations (including both IT and non-IT staff). We stress that these harm tables are a 'snapshot' of harms that ransomware victims may experience. Ransomware experiences can vary markedly, depending on internal and external contexts. Our tables – and analysis – is not comprehensive. However, our exploratory research approach has enabled us to draw an analysis that develops a significant depth and breadth of understanding of the ransomware victim experience. This builds upon the existing research highlighted in this section, and contributes to the filling of pertinent gaps in collective understanding; including across academia, policymaking and other stakeholder contexts.

Research methodology

In order to answer our research question "what harms do victims of ransomware experience and what factors alleviate or aggravate those harms", we created a research process consisting of three stages and touchpoints with participants: semi-structured interviews, book-ended with two workshops. In total, 83 participants were involved throughout the three stages of the research. The inclusion criteria for participants at every stage of the research were as follows:

- Individuals representing organisations based (in whole or substantial part) within the UK that had been subject to a ransomware attack and that could speak to either: the impact of the attack on the organisation and/or the direct effort to resolve the impact of the attack.

- ¶ Individuals with significant professional experience of supporting organisations based (in whole or substantial part) within the UK that had suffered ransomware attacks, for example, through providing: Insurance, Incident response, Legal services, Police/emergency response services, or National/international level policy-making and governmental oversight.

Workshops were performed at the start and end of the interview period as a means to frame, validate and further explore topics. These were collaborative events, designed to use the participants' expertise to bolster, at the start, the set of interview questions; the workshop at the end provided an opportunity to interrogate the analysis performed on the interview data to that point. The choice to use workshops in addition to interviews was made as a means of increasing the rigour of interview question setting and the conclusions made from data analysis. In coordinating a group of experts with different experiences of the issues posed by ransomware in organisational settings, the workshops allowed for debate and discussion to hone the knowledge and understanding of the subject, based on recent professional experience. The use of a combination of individual data collection and wider expert workshops is in keeping with similar previous research such as Mott et al [1] and Parkin et al. [73]. Below we present further detail on each of the three stages.

Following the receipt of ethical approval from our institution's internal/ethics review board, the first workshop was scheduled. To expand upon the methodology's introduction above, the premise of the initial workshop, which was held in November 2022 over Zoom, was to explore the types of harms that the participants had collectively witnessed when supporting victims of ransomware attacks – this was done as a basis upon which to frame the interview questions. The use of the workshop allowed for group discussion and resulted in the refining of ideas over the period of the session, which may not have occurred as organically in one-to-one discussions. For a breakdown of the first workshop's participants and their professional background, see Table 1. It should be noted that four participants from this workshop were subsequently interviewed in stage two.

Table 1: Workshop 1's Participants

Type of Organisation	**Number of Participants**
Cyber security [CS]	1
Digital Forensics and Incident Response (DFIR) [DFIR]	10
Government [GOV]	1
Cyber insurance [CI]	3
Law enforcement [LE]	5
Law firm [LF]	3
Ransomware recovery [RR]	3
Total	**26**

The second stage, semi-structured interviews, was performed between November 2022 and March 2023. In total, there were 42 interviewees; these were sourced initially from the network of the authors and, subsequently, through snowball selection. Interviewees were loosely considered to be

one of three types: representatives of directly attacked victim organisations[3], from organisations that directly support victims during the ransomware process (including law enforcement), and individuals from the government (including policymakers) who focus on ransomware. For a full breakdown of participants by type, see Table 2.

Table 2: Interview Participants (non-victims and victims)

Type of organisation	Number of participants
Crisis communications [CC]	1
Cyber insurance [CI]	3
DFIR [DFIR]	6
Government [GOV]	4
Law enforcement [LE]	3
Law firm [LF]	4
Ransomware recovery [RR]	3
Total (non-victims)	**24**

Type of organisation	Number of participants
Education [ED-VIC]	4
Engineering [ENG-VIC]	1
Financial Services [FS-VIC]	
Foreign Government [FGOV-VIC]	1
Government [GOV-VIC]	1
Healthcare [HC-VIC]	1
Local government [LG-VIC]	2
Manufacturer [M-VIC]	1
Professional Services [PS-VIC]	4
Technology [T-VIC]	3
Total (victims)	**18**

A semi-structured interview process was necessary to ensure the flexibility required to focus upon those issues that were the most important to each participant. Not all questions were asked in all instances. Although the questions were slightly different depending upon the context upon which the participants were being interviewed, for victims in particular, it was considered vital by the interviewing team to enable the discussion to flow in ways that could explore the most important aspects of their experiences. As mentioned above, the questions asked around harms were informed by the findings of the first workshop. For the full list of questions, see Appendix A.

[3] That is to say, participants in this group were employees at organisations that had directly been targeted with ransomware, and not further down the supply chain.

Representatives from organisations that had suffered a ransomware attack were prompted to give details about their organisation, and then details about their experience of the ransomware attack, as they experienced it. As these individuals did not all work within IT, some could not speak in as much detail about the technical implications, but rather were well placed to discuss the operational and wider impacts upon their organisation and its employees (and any other organisations or individuals). Participants were then asked details about the timeline of the harms they recognised their organisation – and those within, and related to, the organisation – suffered as a result of the ransomware attack, and what harms they were. We then probed whether there were harms that they recognised had occurred but were overlooked, whether within the organisation or more generally. Our line of questioning also considered whether there had been any attempts to measure, quantify or otherwise document the impact of the attack on the organisation. If so, participants were asked if they could share the outcomes, and if not, what measures they would consider valuable to use when quantifying the impact.

After this set of questions, representatives from victim organisations were asked about their experience with third parties: who proved to be supportive, and why, and who was not? Were there any aspects of third-party involvement (or lack of involvement) that turned out to be especially beneficial or damaging? What reporting did the organisation perform, and was that process – where reporting was undertaken – easy or difficult? What improvements to the process would they suggest? Would they expect more support from any parties? And what would they have done differently?

Other participants, including third-party support services, law enforcement and government/policy makers had a different version of the questions asked to representatives from victim organisations. In particular, third parties and law enforcement were asked to give answers speaking to their overall experience of assisting victims of ransomware, in line with the topics listed above.

The third stage in the research process was a second workshop. This workshop asked participants to reflect upon the harms and mitigating factors that had been brought up in the interview process and consider whether any further aspects should be refined or explored more, through other interviews (following a similar methodological approach to Hadan et al. [46] and Mott et al. [1]). The workshop had 21 participants, of which two had also been interviewed – for a breakdown of workshop participants, see Table 3. We held the session over Zoom in March 2023, and following a presentation of the findings to date, participants were split into two breakout rooms for further discussion, for a period of 50 minutes. The outcomes of the workshop showed broad alignment with the harms and factors elicited in the interviews.

Table 3: Workshop 2's Participants

Type of Organisation	**Number of Participants**
Academia [AC]	2
DFIR [DFIR]	10
Government [GOV]	4
Cyber insurance [CI]	2
Law firm [LF]	2
Ransomware recovery [RR]	1
Total	**21**

Both workshop sessions (including Zoom chat logs) and all interviews were audio recorded and transcribed, with all identifying features of the participants removed. Following this, they were coded by two of this paper's authors using NVivo 12. The transcriptions were subjected to thematic analysis [45] by these researchers to draw out themes. Following this extremely widely applied analytical method, as refined by Braun and Clarke since 2006, we agreed that the text would be approached in the following ways:

- Analysis would be undertaken deductively, with coding being framed in part by the questions being asked, and the need to focus on non-financial and organisational harms especially, given the prevalence of these harms in previous research.
- Analysis would be latent, not semantic, in nature: although experts in the field would have a precise grasp of terminology and a more detached emotional experience, it was considered likely that victim participants in particular may be unable to explicitly verbalise either technical aspects of recovery or, more generally, struggle to discuss difficult and stressful situations. In this case, the implicit understanding of the participants was deemed to be invaluable, particularly given the absence of such voices from the existing literature.
- Analysis would be constructionist in approach: the sensitivity required to understand and report upon the victim experience would necessarily require using the participant's perception of the situation as the reality of the situation. This was considered especially important given previous literature focused less on the human aspects of the impact of ransomware (as discussed in the literature review), giving the potential for underrepresentation of the physical and emotional toll of such events.

The initial code book was created deductively by one researcher based upon the structure of the interview questions. Both researchers then coded three transcripts using this code book to understand if the codes created were sufficient. After our further consideration, one more code was added; the completed code book can be found in Appendix B. Although Braun and Clarke's approach does not call for the comparison of researchers' codes for similarity, it was considered by the research team that some additional rigour would be provided by doing so. The two researchers worked independently, coming together at the end to compare the differences within their coding. Cohen's *kappa* was calculated to evidence inter-rater reliability: the score was 0.81, which evidences almost perfect agreement [47].

In the next section, participants will be referred to in the following way: interview participants will be referred to by a shortened version of the category labels seen in Tables 1, 2 and 3 (e.g., Cyber Insurance is shortened to CI, so the second interviewed Cyber Insurance professional is labelled CI2. Victim interviewees have had "-VIC" added for clarity in the attribution of comments in the results section). This will be appended with a number based upon the order in which the participants were interviewed. Workshop participants will be treated in the same way, with a W attached to the start of the shortened category label (e.g., W-CI2). Given the sensitivity of the topic being covered, victim participants may be referred to with a high level of anonymity in the results section that follows, in particular, avoiding giving details of the sector the organisation is in. This is to ensure that participants are not inadvertently de-anonymised by details of the circumstances of the attack suffered.

Results

This section presents findings regarding the harms that victims of ransomware attacks experience and the factors that alleviate or aggravate those harms. In sum, the interviews and workshops highlighted important areas of convergence and divergence between the experiencing of harms between victim organisations and the employed staff. Accordingly, we draw on excerpts from the qualitative data corpus to present experienced harms that interviewees and workshop participants highlighted as being prescient. The first section considers prescient organisational-level harms, and the second section considers prescient employee-level harms. At the end of each section – organisation and employee, respectively – we also include a table that lists all the harms that were discovered across the interview and workshop data corpus. Lastly, this section draws on the data gathered to present the range of factors that were identified as either potentially aggravating or alleviating the victim experience. We first focus on three of the most salient factors, namely, (ransomware) crisis preparedness, leadership culture, and communication (both internal and external). This is followed by a table that lists all the aggravation/alleviation factors found across the interview and workshop data.

The harms experienced by the directly targeted organisation

Ransomware is recognised as a severe disruptor

A primary finding from our research was the agreement by participants that ransomware could cause significant harm for organisations: not only can it immobilise organisations, but its continuing evolution means that attacks are swifter and perhaps more effective now compared to the past. The ability to disrupt an organisation's ability to function was discussed by some victims as being swift to arise and potentially fatal to the organisation. One victim at a legal firm described it as "*[an organisation's] number one risk, having gone through that experience … it has to be the number one threat because it's the only thing that can close you down immediately … I think it's that fundamental and existential*" (PS1-VIC). A participant with experience of an attack against a critical national infrastructure (CNI) organisation at the heart of a small country noted that the incident *"totally paralysed the country"* (FGOV1-VIC) causing severe disruptions to governmental organisations at national, regional and local levels.

Those interviewed that worked in supporting the victim's recovery discussed how the relative speed of attacks has increased over time: "*we have older incidents where you have the killchain happening over eight days. Now it's like over hours*" (CI3). This sometimes leads to a level of violent refocus for organisations: *"I think you struggle to find something that is so immediate and has such a cataclysmic effect on a company's ability to trade than ransomware … it happens literally overnight. And everything you relied on yesterday is suddenly no longer relevant and you can't see beyond the next couple of weeks"* (LF4).

In terms of the harms upon the direct organisation, these can broadly be categorised into two blocks: financial and reputational. The financial harms include loss of income due to business interruption (LF4), the cost of remediation (ED1-VIC) – for instance, new systems, staff overtime, third-party incident response services and legal support – and possible future lost income due to foregone future clients and contracts (M1-VIC). Reputational harm could be manifested in the form of lost-trust between the victim organisation and their clients, supply chain, business partners and own workforce (M1-VIC). In this lens, reputational harm appears somewhat linked to financial harms; i.e., a damaged reputation (or fear of a potential reputational damage) is harmful because it can lead to, or exacerbate, prospective financial loss. Nonetheless, the interview data did highlight a debate as to whether financial or reputational impacts are more harmful than the other, with some arguing that financial impacts were more harmful (T2-VIC) and vice versa (CI3). Importantly, this was typically caveated by context-dependency (DFIR7).

In principle, one may argue that harms to the directly targeted organisation could be quantifiable. Whilst some of the harms noted later in the paper – such as psychological stress experienced by staff – may be more subjective, harm-to-organisation could be narratable as overt business costs. However, measuring the severity of harm in overt units can be challenging. Time-to-recover is one way of measuring harm to an organisation. Interviewees highlighted that following a disruptive ransomware incident, an organisation might typically experience an initial crisis phase lasting days or weeks (T3-VIC), and that it could typically take several months for an organisation to return to 'normal' operations (CI1).

The financial cost would be another measurement. One way in which organisations could provide a ballpark figure of overall cost is through the value of their insurance claim (CI1); assuming that they have cyber insurance and choose to make a claim. However, whilst this provides an indication of the insurable losses, it may not necessarily be a true reflection of the actual loss. Organisations typically would make an overall assessment of the cost and either disseminate this externally or internally (GOV2-VIC). Where such an assessment was disseminated solely and confidentially with senior management, interviewees were understandably unable to share the figure(s) with the interviewing team. More broadly, interviewees noted that it was difficult for organisations to identify a categorical figure of the cost of a ransomware incident when conducting a post-event report (FS1-VIC; PS1-VIC). This challenge was exacerbated by other fiscally disruptive events, such as the SARS-CoV-2 pandemic (FS1-VIC).

Harms experienced depend on context

Although the disruption of ransomware was widely recognised by participants, there was sometimes a surprising lack of agreement on how severe the risk was relative to other potential organisational disruptors. This was noted, in particular, in organisations with significant other regulatory burdens, where other existential threats were more clearly defined, as they relate to the organisation's requirement to keep people safe. One interviewee, who had dealt with a significant health and safety incident prior to the ransomware attack, rated the ransomware as less severe (PS2-VIC). A victim from the education sector reflected that "*ultimately, a pupil isn't going to die as a result of a ransomware attack, and therefore it is a lower level of risk, [although] it might disrupt their education*" (ED4-VIC).

This divergence of concern about risks also spread into views as to whether data exfiltration or data encryption was worse for an organisation. Whilst one interviewee noted that *"I think people are probably more scared of the data breaches … because that is something that they can't control … that is more of a major concern"* (LE2), others argued that encryption remained the most harmful, likening its capacity for business interruption to a *"cardiac arrest"* (LF3). One ransom negotiator highlighted that in cases where encryption was a serious issue for the victim organisation, about 70% of such victims would opt to pay a ransom (DFIR6). Comparatively, in instances where only the data exfiltration was a serious issue for the victim organisation, about 30% of such victims would elect to pay a ransom (DFIR6). This roughly aligns with those interviewed victims who would openly discuss paying a ransom: of three in total, one reported paying due to the sensitivity of the exfiltrated data (PS4-VIC), with two paying because it presented the most efficient solution to decrypt affected systems (ED1-VIC; T3-VIC).

Interviewees cited a range of reasons why organisations suffer differently from similar attacks: encryption was significantly more harmful where there could be little tolerance to business interruption, with possible loss of business or the breaking down of supply chains as a result: *"when we look at the sort of the supply chain risks, it's amazing where the problems exist no matter how much planning you do…"* (DFIR2). Exfiltration of particularly sensitive data, however, could result in different harms: costly litigation, a prolonged loss of trust (LF4), or in certain cases, actively putting

individuals in danger where the organisation has safeguarding obligations (DFIR7). In such cases, often it could be only *"small parts"* (DFIR4) of a much larger exfiltrated data set that cause significant concern. Therefore, the problem arises that it is simply not clear what data the actor has access to, and trying to find out that information is extremely hard, even with the insight gained during negotiation. One education sector interviewee explained that:

> [the ransomware actors] started to talk about pupil information. And that's the thing that we really would worry about, because it's all sorts of safeguarding stuff, medical stuff, but in the end, they didn't have that. So we called their bluff … when they started their dark-web page, they had salaries of staff, and that was bad … but they didn't have pupil information to put up. (ED2-VIC)

The lack of certainty around the data that has been exfiltrated also makes it harder to assess which data subjects to notify, and how to narrate the seriousness of the breach with individuals impacted, regulators and the press (W-DFIR1). Additionally, in order to maintain pressure on victims, ransomware actors have been known to lie about exfiltrating data (FS1-VIC); there is also the ongoing concern that exfiltrated data could (re)surface several years after the initial breach, creating questions around liability (DFIR7), particularly if those whose data was lost can evidence harm (W-LF1).

Thus far in the paper, we have presented select organisational-level harms that interviewees and workshop participants narrated as being particularly prescient. Table 4 presents the full set of organisational-level harms that we discovered through our research as linked to the ransomware attack. While we have sought to be comprehensive, other harms may exist that were not mentioned by participants, and not all harms may be present in all cases – there may also be contextual and organisational variables at play. We posit that this table will be useful in informing researchers, policymakers and industry stakeholders about the breadth of harms that can emerge as a result of ransomware incidents. This may also support the ongoing refinement of cyber harm taxonomies [48]. For the purpose of clarity, we have categorised harms as either physical, economic, reputational, or social/societal. This list does not assign any greater/lesser significance to particular harms, and as such, we document harms in alphabetical order.

As noted at the beginning of the Results section, the data gathered highlighted areas of convergence and divergence between the experiencing of harms of an organisation vis-à-vis the staff at the organisation. The next subsection, therefore, outlines a range of harms experienced by employees, including both financial and non-financial. One early relevant observation is that employee efforts to alleviate harms to the organisation can, in some circumstances, lead to employee harm.

Table 4: Harms to organisations identified in interviews and workshops

Harm type	**Harm experienced by the organisation**
Physical	CCTV, fire and/or estate control systems unusable
	Data exfiltrated
	Data files damaged temporarily or permanently
	Decryption keys may not work or may partially work
	Disruption to online presence
	IT infrastructure damaged temporarily or permanently
	IT infrastructure maliciously used as cryptocurrency miners
	IT infrastructure switched offline
	Organisation cannot continue operating and/or goes bankrupt
	Potential contestation between recovery and forensic efforts
	Ransomware may be followed by opportunistic DDoS attacks

	Ransomware may be used to cover up another illicit activity Verbal and written hostility/anger from clients Verbal and written hostility/anger from staff
Economic	Cost of covering sick leave for impacted employees Cost of credit monitoring services for persons impacted Cost of electricity consumption for attacker's cryptocurrency mining Cost of incident response services Cost of IT training Cost of legal services Cost of litigation Cost of lost productivity Cost of mitigation of attack Cost of new replacement IT systems Cost of new services (e.g., threat monitoring and cloud services) Cost of new software Cost of public relations services Cost of ransomware negotiators Cost of replacing staff who leave the organisation Cost of triggering contract penalties due to business interruption Costs from anticipated or unanticipated gaps in insurance coverage Depletion of financial reserves Drawing on credit lenders and/or liquidity teams Fees to access cryptocurrency Increased cost of cyber insurance premium Interruption to payroll operations Jeopardization of a pending acquisition Jeopardization of a pending merger Loss of data can make taxation paperwork challenging Loss of future sales and contract renewals Loss of income due to business interruption Opportunity cost of exertion and diversion of resources Ransom payment Regulatory fines
Psychological	N/A – organisation is an inanimate entity; psychological harms covered in staff harms
Reputational	Attackers use victim IT systems to fraudulently contact clients Clients have less trust in victim organisation Industry peers have less trust in victim organisation Loss of trust within organisation Negative exposure in industry publications Negative exposure in media or social networks Organisation's exposure on data leak sites Organisations in the supply chain have less trust in the victim organisation Reduced net promotion score Regulatory censure Requirement to flag the incident in future audits
Social / Societal	Degradation of workplace culture Exposure of illegal data handling Exposure of malpractice Jeopardization of safeguarding obligations or responsibilities Supporting crime in the event of ransom payment

The harms experienced by staff within the organisation

From an analysis of participants' responses, a range of significant financial and, in particular, non-financial harms are experienced by staff working organisations suffering a ransomware incident. As may be expected, there was a range of immediate, and often severe harms associated with being IT staff or those staff directly responsible for dealing with the immediate remediation effort; however, non-IT staff also reported suffering harms as a result.

Those staff members working directly on incident resolution

Interviewees reflected upon the lack of attention paid to the mental and physical stress that those responding to a ransomware attack within their organisations experience. One interviewee from the education sector commented:

> I think the biggest reflection for me was the human toll on the IT service … the stress from some of the IT colleagues who really understood the detail of what goes on … I think that's probably not spoken about. Because people just think magical IT will come and sort it all out. (ED3-VIC)

The mental stress of handling such a difficult incident is perhaps obviously understandable – and in many cases, participants discussed a rallying together and strong bonding of key members in the face of the incident*: "I think within the IT team , it was … quite a thrill of being into action, do[ing] stuff"* (LG1-VIC). Physically, however, the toll of handling the attack on their organisation had a much more pernicious, and in some cases, longer term, impact on many of the interviewees directly and for others that they knew. Working extensive overtime and at unsociable hours; not eating properly; consuming too much caffeine and/or not sleeping properly (PS1-VIC; T1-VIC). As one victim – who coordinated their charity's response – recalled:

> … I forgot to drink, eat … one of [my team] was hospitalised for a few days, just through not caring for themselves. I had to go for a quick check up in A&E [Accident & Emergency], because my heart palpations were getting a bit out of control. I just drank too much coffee and not enough water. Just trying to stay awake and all that … but you do what you need to do (HC1-VIC).

Some reported physical injuries second-hand; for instance, a law enforcement interviewee reported that: *"one of the ladies I spoke to recently, she was a victim of ransomware and not long after she had a stroke, and she believed that was brought on by the stress and harm that it caused her"* (W-LE7). Others shared their own personal first-hand experience of physical harm. An interviewee attributed their heart attack to the stress and rigour of the incident response that they coordinated (FS1-VIC).

IT staff are not the only integral employees in response efforts: those within victim organisations that also had to make key decisions under significant pressure reported the long-term physical and emotional tolls of doing so (LF3; CI2). An executive of an SME highlighted the severity of the psychological toll that their ransomware event had upon them personally, noting that: *"there was a bit of PTSD [Post-traumatic stress disorder] every time I walked through the office door … I was at times suicidal. I think I came as close to suicide as somebody who would never commit suicide would"* (PS2-VIC).

High stress levels amongst IT staff were so commonplace that some incident response firms had developed in-house confidential trauma counselling capabilities for clients; one incident responder noted that about 20% of victim organisations would take up such a service for their employees (DFIR6). That statistic was largely borne out within interviewed victims: although one victim who coordinated the response at a multinational engineering firm described how the *"PTSD team [brought in] to work with everybody…in the core team"* (ENG1-VIC), other interviewees at the head of impacted organisations were not aware of employees reaching out to the already offered counselling services as part of their employee benefits packages specifically to discuss this*: ά...we've got 24/7 kind of counselling online, phone thing, people can use them. Not sure… I'm not sure… that [anyone did]*" (ED2-VIC). This lack of consideration or interest in the need for psychological support was echoed by those who supported victims through incidents. A legal professional with experience assisting organisations through cyber incidents suggested that *"in the vast majority of cases, it seems to be just like, suck it up and sort it out. And if we don't we are all out of jobs"* (LF4).

Interviewees also highlighted that pre-existing workplace employer-employee dynamics could also feed into the framing of an incident response. This framing, in turn, could influence the breadth and depth of harms experienced by staff. Whilst harms are both objective and subjective, employees and/or employers will have to manage irrefutable logistics. This could be as mundane as ensuring access to food and rest. A microcosm of this was the communitarian versus individualistic dynamics within the workplace. For instance, UK organisations were reported as less likely to have a 'canteen culture' (DFIR2; W-DFIR10) while organisations in continental Europe were noted as having a more prominent canteen culture. We saw this in discussions with incident responders who stated that when they responded to a ransomware incident for a firm where employees expected to be fed, they provided a template incident response – wherein canteen was low priority. In response, the victim organisation would then re-prioritise ensuring the canteen was operational. The organisation(s) defended this as they were conscious that a disrupted canteen would cause significant discontent amongst the workforce (DIR2; W-DFIR10).

One UK victim noted that their health hardship during the incident response could have been partially alleviated if they had been able to use accommodation linked to their employer's building, to rest and consume some food (HC1-VIC). On the other hand, a CISO at a UK manufacturer appreciated the provision of a new freezer with ice cream, which helped sustain colleagues working overnight (ENG1-VIC). An interviewee who coordinated the response to a ransomware incident against a financial services firm noted that harms-to-employees has knock-on effects to the organisation itself; suggesting that the organisation should have offered core IT colleagues garden leave after the brunt of the response was over – but did not – resulting in 'months and months and months' of sickness leave instead (FS1-VIC).

Those staff members not working directly on incident resolution

It is important to note that interviewees highlighted harms to staff that were not integral to the recovery effort as well. Whilst they may not have sustained such severe physical outcomes, stress and uncertainty were commonly reported in having to talk with and try to retain clients without a clear picture of the impact of the attack (RR1), having to ensure vulnerable clients remained safe – or worrying that they would remain so in the face of data leaks (ED2-VIC). Non-IT staff – particularly those working from home – who were updated about the incident response intermittently were reported to have experienced a sense of dislocation, compounded by the challenge of undertaking their routine work (ED3-VIC).

Participants also described the difficulty that having to adopt new working styles posed, whether in the immediate aftermath of the attack or in the longer-term (M1-VIC; GOV1-VIC). A senior manager at a government agency that had been unable to restore its old systems – instead migrating to cloud systems – noted that their staff suffered multi-faceted stress in the aftermath of the incident. One element was, in some respect, akin to PTSD; fear of a follow-up attack and being 'twitchy' about security alerts (GOV1-VIC). The second element was a negative reaction to the new ways of working, and they noted that some of their staff had continued to be frustrated by the loss of old data systems and found the new systems frustrating (GOV1-VIC). In a similar vein, albeit in a different sector, an executive from the education sector noted that their teachers expressed frustration about years' worth of teaching materials being irreparably lost, contributing to some of the teachers deciding to leave the organisation (ED4-VIC). An executive at another organisation noted that staff were passionate about data that they had collected as far back as the 1980s, and expressed frustration this data remained encrypted after the core recovery effort had been completed (GOV1-VIC).

Employees, too, were victims of the attack, as well as suffering the harms to their professional lives. The offer of identity protection cover or credit checking was mentioned as almost routine, and covered, typically, by insurance (CI3). Financially, a wide-range of outcomes were discussed during the interviews: several interviewees highlighted that staff continued to be paid in the normal way during and after a given ransomware incident, even in instances where payroll was impacted (M1-VIC; PS1-VIC). In some cases, the timing of the incident was fortunate; for instance, payroll had just been finalised prior to the encryption event (ED3-VIC; T3-VIC). However, in other cases, it was such that employees did experience direct disruption to their pay (LG2-VIC). In a particularly severe ransomware case involving impacts to the education sector, teachers were not paid for several months, contributing to issues with mortgage and automobile payments (FGOV1-VIC).

Table 5 presents the full set of employee-level harms that we discovered as associated with ransomware attacks. Similar to Table 4, the table is not universal to, or definitive of, all attacks and contexts; however, it does present a complete outline of the employee-level harms that were present in our data. We expect that this output will be useful in informing stakeholders about the breadth of employee harms that can emerge as a result of ransomware incidents. We have categorised harms similar to Table 4 and also present them in alphabetical order.

Table 5: Harms to staff identified in interviews and workshops

Harm type	
Physical	Breaching of health advice (e.g., COVID-19, SARS-CoV-2) isolation thereby increasing personal risk Death Lack of adequate exercise Lack of adequate nutrition Lack of adequate sleep Minor illness (i.e., heart palpitations) Over-consumption of caffeine Serious illness (i.e., heart attack or stroke) Weight changes
Economic	Cancellation of annual leave or holiday plans Economic risk to personal assets (i.e., for a micro-SME owner) Increased future risk of fraud Loss of / interruption to salary Productivity impact

	Redundancy
Psychological	Anger Confusion Embarrassment Frustration Guilt Isolation Loss of self-confidence Post-traumatic stress disorder (PTSD) Self-doubt Shame Stress Suicidal thoughts
Reputational	Clients have less trust in victim organisation's staff Exposure of individual in media or social networks Industry peers have less trust in victim organisation's staff Loss of trust within organisation Supply chain have less trust in victim organisation's staff
Social / Societal	Disruption to family routine Inability to take bereavement leave Inability to undertake childcare duties

What factors alleviate and aggregative the harms experienced?

Throughout the interviews, a range of factors that made the experiences of victims better or worse were explored. Although, in many of the interviews, it was made clear by participants that some of the outcomes – particularly positive ones – were often in part due to luck (for example, having just run payroll immediately before the attack), many others stemmed from decisions, typically, about the importance of managing cyber security and resilience within the organisation beforehand. Three core aspects that could make outcomes better – or worse – are discussed below: the right forms of preparedness, the importance of appropriate leadership culture, and the role of communication. These were the factors that were highlighted by interviews and workshop participants as being most pivotal in influencing the victim experience. In addition to the presentation of excerpts relating to these three core aspects, this section also presents a table that includes the full range of 'victim experience' influence factors that were present within the data corpus.

Preparedness

Crisis planning and preparedness were cited as important pre-ransomware event influences on alleviating or worsening the experienced harms. An IT Director from the education sector suggested that their workplace culture was a positive one, and that colleagues were well-supported during and after their ransomware event (ED3-VIC). However, they highlighted that:

> we had a business continuity call early on. People from outside of IT were saying we're going to do a business continuity plan, and I can vividly remember this one person saying I'm gonna work on Excel and email things around. I'd probably worked too many hours at the time, quite tired and quite drained, [and I said] `You've not got the concept of no IT. There is no email. There is no Excel. Think pencil. Think paper.' (ED3-VIC)

An insurer described the same phenomenon:

> it's down to preparedness. So, have we understood what the likely impacts could be on us, how are we prepared for that? Do we think we've got the right things in place? Those [prepared] organisations, it's starting to come out in the wash now, that they tend to respond better and recover quicker, [have] less impact, than those where you've got some alphas running around, beating the chest, thinking they know, and actually are causing more harm than good. So I think that governance and culture is probably the thing that gives you the indicator as to what side they're going to land (W-CI3).

An element of preparedness allows for the ability to stop and think. Victim participants who took time to understand the issue did not report paying the ransom. From the victim's point of view, there were typically two reasons for this: paranoia that their existing IT ecosystem could still be compromised and wanting to take the time to either clean the machines fully or replace them with new ones (ED3-VIC). Secondly, the ransomware incident provided both an opportunity and a rationale for IT upgrades that had been overlooked or were scheduled to otherwise be implemented at a later date (HC1-VIC). In this sense, the 'slow and considered' recovery approach sought to mitigate against potential future harm by reducing the likelihood of re-infection and bolstering future resiliency. From an incident response point of view, the more controlled and slower the response, the less likely the chance of paying because the longer the time spent on negotiating, the more the advantage plays into the victim's hand**s** (RR3).

Preparedness comes in different forms. In many cases, organisations had already had to deal with major technological changes in order to manage the stay-at-home and lockdown orders associated with the SARS-CoV-2 pandemic. Working from home lessened the amount of 'noise' that could be generated by on-site colleagues and clients. It also meant that the recovery of infected machines could take place in a measured way; for instance, with colleagues invited to come on-site at scheduled appointments for 'laptop clinics' (ED3-VIC). Additionally, the workplace restrictions during SARS-CoV-2 (COVID-19) for office staff meant that colleagues were more accustomed to home-working and home-IT provision than they otherwise might have been (ED4-VIC). This meant, for instance, that colleagues had already adopted cloud services and were accustomed to them, rather than using the internal hard drive on their individual office machines (ED3-VIC). A senior manager at a public body noted that:

> … we were building capacity to allow people to work from home, and I'm going to say by good design rather than good fortune, we had a video platform which was completely separate from our systems, and that was the method of communication [during the incident]. So, having to deal with a large business continuity issue of the pandemic actually equipped us to be able to communicate with each other. (GOV2-VIC)

Additionally, rapid workaround decisions may help to facilitate the recovery process, particularly in cases where traditional means of communication are either inoperable or may still be accessed by the ransomware actors. Several interviewees highlighted that they used alternative communication methods, including WhatsApp, Signal and/or private email (ED1-VIC; ED2-VIC; ED3-VIC; ENG1-VIC), with some also using rapidly spun-up internal or third-party temporary email domains (ED1-VIC; ED3-VIC). In a similar vein, a Senior Security Officer noted that: *"we had people buying Chromebooks by the bucketload. That was the way forward; everybody getting a Chromebook to help get access to our M365 environment, and that's how we were communicating and talking to people"* (ENG1-VIC; also ED4-VIC).

Cyber insurance was commonly discussed as another important means of preparedness, alleviating particularly the financial element and the provision of vetted incident response services (PS4-VIC; ED3-VIC). A cyber breach lawyer noted that from their experience of working with clients, those clients

who had cyber insurance typically fared better and were under less pressure to lay off staff during or after the incident (LF3). A lawyer at a victim organisation recalled that:

> the firm had the benefit of cyber insurance, and that was helpful, if nothing else, because we were able to act without worrying too much about the cost … I think the most useful thing about that and getting the expert help quite quickly was that we were able to deal with people that deal with these things all the time … for me, [cyber insurance was] absolutely pivotal, vital that we had that. If we didn't have that insurance available, I don't know where I would have started to find the right experts. (PS1-VIC)

A Director at a micro-SME had purchased cyber insurance on a whim but found it invaluable during their ransomware incident, both financially and in relation to the provision of expertise (PS2-VIC). Asked how they would have fared if they did not have this policy, they replied that *"the business would have closed and our house would be on the market"* (PS2-VIC). The access to the right professionals afforded by cyber insurance was repeatedly considered to be crucial: "*[T]here is no kind of money you could put on the [assistance provided by the insurance], to be honest*" (T3-VIC). Whilst victims consistently praised the value and quality of incident response that could be accessed through insurance, in other instances, trying to find the appropriate support could be less successful. There were some instances described by interviewees where an incident response company may either be of poor quality or be poorly aligned with the sector, format and IT infrastructure of the victim organisation. An incident responder described this as a:

> huge problem. I think in the past 6 months, maybe 50% of the ransomware cases we picked up, we're the second firm in … it's just the experience bit. It's the churning through high case loads that lead you naturally to the most efficient and effective path … [we've] seen some awful, awful aftermaths of either bad breach counsel, bad public relations, bad incident response, even bad recovery. (DFIR1)

They added that *"almost always"* the issue derived from the victim having called upon their existing partner; for instance, their managed service provider (DFIR1). This was a common theme raised by incident response interviewees (CC1), with some making reference to inexperienced and/or inadequate vendors operating in the market (W-DFIR1). Another interviewee noted that panicking victim organisations faced a challenge, *"in the midst of a crisis, trying to pick your trusted advisors and whether you should trust that organisation is very challenging"*. It was also noted that victim organisations could be reticent about the high costs of incident response and could be keen to end the contract as soon as the core recovery was complete (W-CS5; W-CS6; T2-VIC), cutting short the possibility of a full forensic investigation (T2-VIC).

The next section outlines the role of positive/poor leadership cultures. This refers to the working environment within an organisation, particularly with respect to the nature of the existing interaction between an organisation's leadership and its wider staff members.

Leadership culture

Thoughtful, experienced leadership culture, and a corporate understanding of the value of cyber security, perhaps unsurprisingly, often led to more successful outcomes: " … the least successful [organisations] are the organisations with maybe immature leadership or not skilled leadership … they're not used to having to deal with this sort of stuff" (DFIR1). The less robust the leadership culture, the more likely that employees may try to blame others, typically leading to poorer outcomes (LG1-VIC). The extent to which the Chief Information Security Officer (CISO) or equivalent role was considered to be a significant part of the senior leadership of the organisation was also mentioned in interviews:

> ... has the CISO been able to get desktop exercises set up where people actually start to understand that ransomware is not a cyber problem. And if [the board are] unwilling to listen, they're unwilling to do X, Y, Z, then the writing is on the wall. It's just a matter of when, whether it is ransomware or something else. (FS1-VIC; also DFIR4)

Additionally, it is important that the CISO has a rapid and effective communication channel with senior leadership to convey information and receive guidance on decision making. Interviewees discussed examples they had seen where the CEO of the organisation would not return the calls of the CISO, exacerbating the issues caused by the attack (CC1). Data Protection Officers (DPOs) and CISOs were also described by some as having the technical understanding to handle the situation, but not having the management support to handle the psychological impact of being the key person dealing with an existential threat to the organisation:

> …psychologically, [the CISO] was nowhere near [capable]. And it was this one guy in the middle who was the fundamental access point for all of the activity. [H]e was kind of on his own, not doing great at all. And I would be really surprised if this was uncommon. I've seen it a handful of times. (DFIR4)

Some participants noted that a crisis such as a ransomware attack could be a catalysing moment – for good or bad – depending upon the ethos and sentiment within the organisation at the time of the event. Ergo, pre-existing discontentment with management could be exacerbated by the disruption caused by a ransomware incident. One interviewee at an attacked legal firm put it accordingly:

> I think it is very easy to underestimate how important your culture is … the stronger culture you have, the more coherent, the more resilient that business will be to something like this happening … whereas internally, if you already have a poor culture, you have people that are quite disgruntled … then you're particularly vulnerable to this having a disproportionate effect on morale because morale is already a bit bruised … morale and culture can't be replaced. (PS1-VIC)

In places with poor existing morale, the attack could be a crystallising moment when staff decide to leave. In effect, the ransomware incident and response became the 'straw that broke the camel's back' moment. This could be organisation-wide, or specific to a particular team. The core IT team, which is likely to bear the brunt of the incident response workload in the initial weeks, are particularly vulnerable to pressure. An interviewee recalled:

> I remember one call when it just emerged that the CISO was a real tyrant. And you know, it was this event and their poor handling of it that was the straw that broke the camel's back … like four [IT staff] left straight after the worst of the incident was over. (CI3)

Leadership culture is, arguably, an a priori factor that exists before an incident emerges; although a crisis such as ransomware can exacerbate existing shortfalls in this culture as well. This, in turn, can influence the staff experiencing of harm(s), hinder the efficiency of the incident response, and lead to legacy concerns; for instance, the costs of replacing staff who have left. Reminiscent of the 'canteen culture' discussed previously (DFIR2; W-DFIR10), the nature of the leadership culture pre-incident tacitly feeds into the framing of the incident response. Senior and executive management will, understandably, want to prioritise organisational return-to-business. However, as the interview and workshop data highlights, pursuing this at the expense of employee wellbeing could, in some contexts, contribute to worse employee experiences. This can have knock-on effects for the employee-employer dynamic that can leave legacy issues for the organisation overall.

Communication

Communication – both internally, within an organisation and externally, with the supply chain and clients – was important in terms of mitigating or exacerbating harms experienced by the organisation and its employees. This is not to say that opacity *or* transparency uniformly alleviates/worsens harms. The scope for differing communication strategies to impact experienced harms is likely to be context-dependent. The combined internal and external communication strategies must carefully navigate multiple channels of harm mitigation, for instance, including but not limited to: controlling legal liability concerns (LF1); dampening possible media scrutiny (CI); reassuring staff, clients and supply chains (ED3-VIC); as well as supporting effective decision-making and the best-use of available resources (HC1-VIC).

It was commonly reported through the interview corpus that organisational victims of ransomware restrict communication about the incident, both internally and externally (HC1-VIC; M1-VIC). Outside of the core IT response team and core senior decision-makers, other colleagues may be left in the dark as to what has occurred, and what the recovery plan is (ED3-VIC). This can have a significant impact on their activities and their sense of disconnection both with their organisation, their clients and their supply chain. A project coordinator at a manufacturer recalled how:

> so the customers were phoning up, all the phones were ringing … but we're not allowed to say to anybody, oh, it's because we've had a cyber attack, and all our things are offline. So everyone's just having to make up bullshit, … still now, we're not allowed to talk about the cyber attack. So customers just stopped asking us, because they were getting nonsense. (M1-VIC)

This was a source of frustration for the coordinator, the sales team(s), and the clients, who themselves were reading about the incident in external media. From the organisation's perspective, an inability for wider staff to undergo their everyday tasks has an impact on productivity and a sense of belonging/utility at a time of organisational crisis (RR; GOV1-VIC). Navigating transparency versus opacity was cited as a particularly challenging element of ransomware crisis management. An incident responder put it accordingly:

> you tend to have two classes of crisis response. You take someone like British Airways, where an event happens, it's clear that there's something going on. But they say nothing to nobody. They don't tell their staff, they don't tell their supply chain, they don't tell their clients. They pretend like everything is fine, when clearly everything is not fine … and then on the flip side, you've got Norsk Hydro who get hit with the attack, and within 24 hours they're literally hosting videos on YouTube of their cyber teams working to recover … they are 100% transparent … I mean, apart from legally sensitive subjects, they're sharing everything (DFIR3; also DFIR5; W-DFIR5).

One area where communication is required, but rarely with a longer-term positive outcome for the victims, was to regulatory bodies – and in particular, in the UK to the Information Commissioner's Office (ICO)[4]. The interviews seemed to suggest that it was commonplace for victim organisations to notify the ICO – in a timely fashion – that they had experienced a data breach (DFIR1; RR1; ED3-VIC; HC1-VIC), although there was some suspicion that organisations may avoid reporting if they believe they could get away with it (LE1). A claims professional at an insurer suggested that nine times out of ten victims would usually contact the ICO (CI1). It was also highlighted that the perceived need to notify the ICO within 72 hours with information about the breach – when not much information may be available – contributed to significant stress for victim organisations (W-CS6). Formal legal supervision, incident response supervision and/or insurance oversight were cited as useful for making a measured and considered notification to the ICO (W-LE1; HC1-VIC; T3-VIC).

[4] The Information Commissioner's Office (ICO) is an executive non-departmental public body that regulates information rights, data retention and privacy in the UK. It is sponsored by the Department for Science, Innovation and Technology.

Fines for loss or potential loss of personal data were not considered to be common by interviewees. However, one prominent finding was that ongoing exchanges of letters with ICO could continue taking place months and years after the event (PS4-VIC; LG1-VIC). A director at a public body described their ongoing ICO case – still open years after the event had taken place – as a "*Sword of Damocles"*, to the extent that *"I think if I was in a private sector business, I would pay [the ransom], and I would not let the ICO know and try and just make it go away really quickly"* (LG1-VIC). An executive from the education sector was more critical and highlighted that:

> the ICO [did not help]. The[y] bombarded us with letters, with multiple questions, and we were treated a bit like we were British Airways or someone. Our team was trying to recover from this, and in the end, I think we sent back 70 pages of answers to the ICO. It was just constant … we've yet to hear back from them. (ED2-VIC)

A cyber breach lawyer confirmed that they were seeing many instances where ICO cases where taking a significant amount of time, contributing to additional distress for the victim organisations (LF4). They attributed this to funding and/or staffing issues at the ICO (LF4). An investigation that took one year was described by a victim as relatively quick (GOV1-VIC). Another victim noted that two years on, their ICO case was still outstanding, and that in one exchange:

> there were 63 supplementary questions. We went through the whole lot and about six months later, they came back with seven further questions, five of which we'd already answered … I don't know if they're going to come back with a massive fine that we have to pay or a big public statement that will then mean we've got to rehearse all of this again with our stakeholders … I would quite like them to get on with it because it was now two years ago. (ED4-VIC)

Drawing on the interview and workshop data, it is apparent that there are a range of factors that can either alleviate or exacerbate the experiencing of harms. Preparedness, leadership culture and communication were particularly prominent. Within these categories, there are a range of factors over which the victim organisation may have varying degrees of control before, during and after a ransomware incident.

To complement the preceding presentation of data relating to preparedness, leadership culture and communication, we present a full range of factors that serve to alleviate or aggravate the experiencing of ransomware harms below in Table 6. Again, this table is not universal and is context/organisation-dependent, but it presents all the alleviation/aggravation factors that were presented throughout the interview and workshop data. For clarity, we divide the table between pre- and post- incident factors. We also do not ascribe significance or frequency to individual factors, and instead list the factors in alphabetical order.

Table 6: Factors that alleviate or aggravate victims' experiencing of ransomware harms

Alleviation before incident	**Alleviation after incident**
¶ Adoption of distributed working environments ¶ Appropriate communications (internal and external) strategy ¶ Appropriate cyber security, which inhibits the attack or reduces levels of access ¶ Appropriate technical resiliency, i.e., viable and regularly updated backups	¶ Appropriate communications (internal and external) strategy ¶ Attackers are intercepted, facilitating early containment ¶ Calming or experienced voices in the room; i.e., veteran or ex-police staff at a victim organisation ¶ Core response staff are (or can be) rotated

¶ Core business systems can continue functioning with IT; i.e., manufacturing Operational Technology (OT) can run offline ¶ Cyber insurance ¶ Existing victim organisation(s) have previously shared their experience ¶ Good knowledge of IT estate (i.e., network diagrams that are held in analogue format) ¶ Good leadership ¶ Good preparation, e.g., understanding that ransomware can be an 'everything' problem, not just an 'IT' problem; wargaming a ransomware incident ¶ High employee morale ¶ IT system is more challenging for threat actors to navigate, e.g., bespoke systems or systems that are too old to quickly deploy malware ¶ Knowledge of what data is held and on which systems, and any unnecessary data is removed ¶ Luck ¶ Organisation does not hold sensitive or safeguarding data ¶ Pre-existing resiliency in work practices, as a result of SARS-CoV-2 work-from-home policies ¶ Ransomware event occurs at an 'ideal' time; e.g., a school holiday period where operations are minimal (this is context-dependent) ¶ Robust business continuity plan and having plan accessible in various formats (e.g., analogue) ¶ Simple IT estate; replacement laptops can be purchased (i.e., micro-SME) ¶ Strong corporate culture ¶ Wider society has become more accustomed to data breaches ¶ Workplace IT restrictions.	¶ Counselling services offered to staff ¶ Cyber insurance ¶ Employee welfare considerations are taken into account ¶ Existing victim organisation(s) can be contacted to share their experience ¶ Expedited access to expert help ¶ Expert help in guiding engagement with regulatory bodies ¶ Good employee support ¶ Good leadership, and as appropriate, leadership listen to advice from IT staff ¶ Good preparation ¶ Luck ¶ Negotiations with threat actors are handled strategically ¶ Protection provided by legal wraparound ¶ Ransom payment resolves the problem; i.e., ransomware key is viable and ransomware operator has a low or zero percent re-offend rate ¶ Ransomware actors appear not to put data on a leak-site, or the data that they have is not sensitive ¶ Ransomware actors are inexperienced and/or accept a low ransom offer ¶ Rapid acquisition and rollout of workarounds (i.e., temporary email domains, WhatsApp groups, Chromebooks) ¶ Robust business continuity plan ¶ Slow and considered recovery approach ¶ Staff or leadership able to share their experiences with peers, reducing stress or trauma; also, positive feelings when a future attack against a peer is prevented due to sharing ¶ Strong corporate culture ¶ Successful separation of containment and recovery operations ¶ Swift and/or uniform agreement not to pay a ransom ¶ Unconventional / possibly illegal solutions solved the problem inexpensively; e.g., commissioning hacking of the ransomware operators (this item is included for completeness, we are not advocating illegal or unethical factors).
Aggravation before incident	**Aggravation after incident**
¶ Bad leadership ¶ Bad luck ¶ Complex IT estate; including systems that were not designed to be switched off or taken offline	¶ Antivirus software attacks the decryption key ¶ Attackers are not intercepted ¶ Bad leadership ¶ Bad luck

¶ Disgruntled employees ¶ Inadequate business continuity plan ¶ Inappropriate communications (internal and external) strategy ¶ Inappropriate technical resiliency (i.e., backups are not deployable or can be infected) ¶ Insufficient cyber security ¶ Insufficient preparation ¶ Limited knowledge of IT estate ¶ Limited knowledge of what data is held and on which systems, and it transpiring that unnecessary data has been retained ¶ Not possessing a set of trusted advisors ¶ Organisation has complex IT setup; for instance, many virtual machines (which may be irreparably destroyed by some forms of ransomware) ¶ Poor corporate culture ¶ Ransomware event occurs at a particularly impactful time; i.e., an impending merger or an educational exam period.	¶ Core response staff are not (or cannot be) rotated ¶ Delay in engaging third parties for support ¶ Disagreement about whether to pay a ransom ¶ Employee resignations ¶ Employee welfare conditions are not taken into account ¶ Employees blaming others/each other ¶ Engagement with inadequate third parties for support (e.g. breach counsel, public relations, incident response, recovery) ¶ High cost of incident response ¶ Inadequate business continuity plan ¶ Inappropriate communications (internal and external) strategy ¶ Insufficient preparation ¶ Lack of engagement with the necessary regulatory bodies ¶ Lack of support from executives ¶ Legal wraparound becomes prohibitive ¶ Negative feelings and guilt when a peer suffers a future incident ¶ Negotiations with threat actors are handled poorly (i.e., Chief Financial Officer (CFO) conducts negotiation) ¶ No immediate access to cryptocurrency; hassle of buying in small amounts and handling fraud checks with bank(s) ¶ Not possessing a set of trusted advisors ¶ Notify ICO too rapidly and in haste ¶ Other ransomware actors opportunistically try to penetrate systems ¶ Poor corporate culture ¶ Poor separation of containment and recovery operations ¶ Ransomware actors attempt further disruption; i.e., DDoS attacks ¶ Ransomware actors cold-contact staff and/or clients ¶ Ransomware actors place sensitive data on data leak website ¶ Ransomware actors refuse to negotiate a lower payment ¶ Ransomware is poorly coded, leaving files or systems irretrievable ¶ Regulatory bodies exacerbate harm by being slow or inept (e.g., ICO taking months to respond, ICO asking questions that have already been answered in prior letters of exchange) ¶ Staff or leadership unable to share their experiences with peers, exacerbating stress or trauma

	¶ Staff trauma or hardship not acknowledged.

In the Discussion section, we draw out pertinent points for our understanding of prominent and nuanced ransomware-related harms, as well as how these can be moderated; particularly from the perspective of organisations.

Discussion

Our interviews corroborate widespread reporting that extortion of encrypted files/systems and exfiltrated data can cause significant financial and reputational harms to victim organisations [49, 50, 51]. However, the data also highlights a nuanced harms landscape, where both organisations and their employees – both IT and non-IT – can suffer. Our research question is: What harms do victims of ransomware experience, and what factors alleviate or aggravate those harms? As such, this discussion section analyses three core areas.

Firstly, we consider the way in which interviewed participants highlighted less commonly discussed harms. This takes into account some organisational harms, but necessarily reflects upon the employee experience in significantly more detail. Secondly, we draw out the potential significance of a range of internal and external factors – before and during an incident – that appear to have a capacity to either mitigate or exacerbate the experiencing of harms. Lastly, we consider the role of third parties and their potential to alleviate harms or, in some cases, aggravate harms. This analysis seeks to offer useful insights for organisational ransomware preparedness and crisis management. Whilst it is, of course, not possible to develop a comprehensive counter-ransomware roadmap within the space of this article, the findings can provide insight into less-widely reported harms and factors entailed in ransomware incidents. Identifying the range and scope of harms is a crucial first step in understanding how best to mitigate against the risks associated with ransomware, not only by management teams within individual organisations, but also in terms of national guidance and policymaking.

Ransomware harms are nuanced and not limited to the organisation itself

Interviewees were clear that not all ransomware attacks affect organisations in the same way; neither do such attacks only affect the financial standing and reputation of the organisation: they also harm employees in differing ways.

The severity of a ransomware attack to an organisation depends upon the goals and other expectations of the organisation itself. Although, of course, it is clear that business interruption is almost always problematic, and data exfiltration can lead to regulatory, legal and financial implications, some interviewed victims appeared relatively sanguine in the face of the attack. This was particularly the case where participants had experience of dealing with other regulatory regimes with stark punishments for non-compliance, and where non-compliance could involve severe injury or worse for affected individuals. That is, however, an extreme contrast that other victims may not have experienced. In particular, the stress and damage wrought upon individuals responsible for small organisations – where the line between being a going concern and losing everything is very thin – was very clear in the interview data.

Above the SME level, employees exhibited the same sort of stressors, not just senior management. Importantly, it is crucial to note that all employees could be impacted – in shared and differing ways – and that harms can extend beyond the core crisis management period. Prior reporting has, arguably, focused on two core employee harms. Firstly, the possibility of staff layoffs – possibly including C-Suite members – resulting from a ransomware attack [52, 53]. The data corpus corroborated this, with some interviewees reporting that they either worked at, or knew of, organisations that experienced staff layoffs. In some instances, it was highlighted that employees resigned from their organisation – citing the ransomware incident as a factor – even where there was no pressure from the organisation for them to leave. In other instances, organisational pressure prompted staff to resign; this appeared particularly prominent for IT staff, who risked – fairly or unfairly – enduring the most blame for the incident and its handling.

Secondly, it has been reported that sensitive employee data can be exposed through data exfiltration [54]. This was, again, remarked upon as being true in a number of cases, although almost with an air of resignation. Organisations aware of such data loss seemed to have worked to provide relevant services to mitigate as much damage to employees as possible – but the actual impact on interviewed participants appeared to be minimal.

It is insightful that these two particular harms were *less* frequently cited in the data corpus compared to other, to date largely unreported, harms, and were considered by interviewees to be less significant than other harms that they had suffered. The most prominent staff harm cited by interviewees was 'stress', which could contribute to psychological and/or physiological ailments. This was particularly acute for the staff who either handled an incident remediation or whose core duties were otherwise significantly impacted by the event. This suggests that psychological harms may be an intrinsic risk for staff who are exposed to ransomware events. This may enable comparisons to other high-stress workplace exposures; for instance, the recorded psychological harms experienced by security operatives, emergency responders and bank personnel [69, 70, 71, 72]. Indeed, it may be possible to learn from these more established fields as we seek a better understanding of the harms from cyber-attacks such as ransomware.

Whilst the harm was particularly acute for IT staff during the crisis management phase, in many cases resulting in physiological impact, all staff could experience stress either directly (i.e., they cannot undertake duties because of system inaccessibility) or indirectly (i.e., confused or exasperated by poor communication within the organisation). Additionally, direct or indirect ransomware-induced stress could extend far beyond the resolution of the incident from an organisational perspective. For instance, whilst an organisation could have returned to business-as-usual, its employees could still be suffering or showing symptoms that could be PTSD or similar conditions months or even years later. At a lower level, interviewees also discussed the need to integrate new processes and procedures to bolster the resiliency of the organisation without additional resources, leading to longer-term risks of dissatisfaction and potential burn-out.

Of course, it is not revelatory that a ransomware incident would contribute to stress and psychological or physiological harm within the workforce at an organisation [28, 30]; it may implicitly be assumed that a crisis would entail stress and human harms. Nonetheless, interviewees often emphasised that the stress-related harms were 'overlooked' whilst the crisis effort was underway, and that more effort should be made to understand the stress-related harms both within organisations and wider ransomware-related discourse to improve its management. Importantly, whilst some interviewees noted that their C-Suite would typically care first and foremost about the profitability of their organisation, hence overlooking 'human' harms, others rationalised that their employers *did* or *should* more proactively seek to alleviate human harms, because not doing so would entail business costs. For instance, mitigation measures could lessen the likelihood of disgruntled staff leaving (which could

implicate business disruption and/or hiring costs) or overworked staff taking sick leave (again, implicating business disruption and/or cover costs).

Organisations can take measures to reduce ransomware harms in advance of, and during, an incident

Another finding from our research is that the scale, scope, and experiencing of harms can be influenced by a range of internal and external factors. Some of these factors are feasibly within the (relative) control of the organisation; offering potential scope for immediate actions to prevent harms. Interviewees generally agreed that the wide range of commonly reported best practices for organisational cyber security would (or should) help to minimise the impact of attacks [18, 55]; for instance, segmented backups, regular patching cadence, cyber awareness training and so on. Importantly, however, without dismissing the significance of technical cyber security, the interviews generally paid greater attention to broader preparedness and crisis management culture.

Business continuity planning and stress-testing can assist IT and non-IT employees – as well as senior leadership – to identify potential issues in an exercise rather than a hostile incident. Wargaming has long been suggested as a means of working through the potential real-life impact of otherwise slightly intangible cyber business continuity threats [56]. Interviewees were clear that the traditional suite of business continuity planning, typically looking at physical, rather than digital, threats, typically required ad hoc, snap decisions and difficult conversations about the limitation of access to resources and tools. Common stop-gap solutions were the creation of WhatsApp (or equivalent) messaging channels for key stakeholders and decision-makers, and/or the purchasing of cloud-based systems such as Chromebooks for staff needing access to files or systems. Having to react, rather than falling back on predetermined plans, was typically considered by interviewees – particularly incident responders – to lead to poorer overall outcomes.

The importance of carefully considered communication in the immediate aftermath of an encrypting ransomware event is clear. This is both a technical issue (i.e., how to communicate without any of the traditional methods available) and a narrative issue (i.e., how, and what, to communicate with employees, clients, supply chains and regulators). The challenge of narrative formation was often compounded by lack of clarity about the incident in the initial days of the event. The impacts of this not only lead to external confusion and frustration, but also internally, amongst those employees who are not within the remediation effort but have been impacted by restriction on their daily responsibilities. Nonetheless, stress-test exercising could help an organisation to identify a range of possible strategies for communicating internally and externally, varied in terms of the severity and nature of a hypothetical ransomware incident [57].

With respect to wider third-party influence on the victim experience, two particular third parties stood out as having a prominent potential to alleviate negative experiencing of harm: incident responders and cyber insurers. Our interview data supported existing literature that has identified the significant role that incident responders can serve in the core crisis phase [18], helping to provide forensic support, cut off the threat actors, identify a plan of action, provide short-term workarounds such as a temporary domain or email server, and, importantly, reduce the pressure on an organisations' IT and non-IT staff by providing their broad experience of handling multiple ransomware cases. The interview data also corroborated existing research on cyber insurance vis-à-vis ransomware [58, 1]; cyber insurance provided both a pool of capital and rapid access to a vetted incident response ecosystem, including technical incident responders, legal firms, PR firms and negotiators. The benefits of this access to capital and expertise may be greatest at the SME level, where internal resource availability

is most limited. Large multinational organisations may have sufficient capital and expertise on hand and may also value internal control of the incident and recovery.

An effect that was necessarily top-of-mind for many interviewees was that of their organisation's reaction to the working-from-home obligations, and knock-on impacts of the SARS-CoV-2 pandemic. The pandemic added complexity to organisational cyber security and increased the attack surface of many organisations [59, 60], but interestingly, our findings suggest that the altered working practices also presented possible benefits. Work-from-home policies – mandated by the government at the time – meant some victim organisations had a lower headcount on-site, and increased dependence upon third-party cloud services which could often be relied upon, reducing 'noise' during the crisis phase. On the other hand, non-core IT staff who were off-site may have felt a sense of dislocation, particularly if the incident meant they could struggle to perform their normal duties. IT staff, too, reported some positive aspects from the sudden ability or necessity to work from home, offering the ability to ensure seeing family and provide some element of downtime not possible when working extremely long hours at the office.

One thing that must not be understated, however, is that all the planning and futureproofing in the world may not help an organisation as much as luck, in some cases. Victims repeatedly referred to elements of luck in their experiences that sometimes had significant impacts on the overall outcomes. Spur of the moment decisions to buy insurance, having just run payroll before the attack commenced, having already migrated some services to the cloud: all of these were described by victims and provided one less thing to worry about.

External factors can be significant

The role of good incident response has been mentioned as a pivotal source of help for victims. However, both victims and incident responders highlighted the damage that inexperienced and inappropriate incident response can create. This may typically occur where an organisation experiences a ransomware incident and, out of necessity, brings in a firm that cannot provide appropriate services - an MSP or hardware vendor – or one that does not align with the victim organisation (i.e., their forensic or recovery tools may not work with the victim's infrastructure). Where this is the case, the inexperience of misalignment may unnecessarily prolong incident response, as the impact of inadequate action will need to be unpicked by subsequent incident recovery firms brought in to deal with the attack. This prompts some considerations.

Firstly, as part of forward-planning crisis preparedness, if they are commissioning incident responders themselves, organisations should – where possible – stress test the experience and alignment of potential third-party incident response firms; especially if their OT or systems are relatively unconventional. However, small organisations may not necessarily have the expertise to make a thorough assessment, and it may be useful to offload this to experienced third parties. Cyber insurers should continue to review the makeup of their panels [61, 1]. Additionally, the NCSC's Cyber Incident Response Level 2 scheme [62] will – subject to take-up – provide a useful vetting resource for SMEs who need to source incident responders directly.

Finally, the concern regarding a long-term legacy of data breach was rendered into a pressing and tangible financial and reputational reality for victim organisations through real or perceived pressure from the UK's data protection authority, the Information Commissioner's Office (ICO). The lack of resourcing of the ICO is established in prior reporting [63], and our interview data corroborated this as contributing to a 'Sword of Damocles' effect for ransomware victims. In essence, victim organisations who notified the ICO frequently – although not always – found that they had to engage

in intermittent exchanges of letters with the ICO lasting an indeterminate period of time. This exchange of letters could continue long after the incident had been resolved. As such, this could leave the victim organisation unsure as to whether there would be an impending fine or statement from the ICO or, indeed, whether their case had slipped from the ICO's radar. With the overhanging possibility of a fine or reprisal, the regulator's lag period may add a material dimension to the challenge of closure following a ransomware event, prolonging harm(s) for the organisation and its staff. Conversely, a speedy conclusion from the ICO could bring forward closure for victims or at least serve as a source of reassurance.

Ultimately, whilst the ICO provides a vital service as a regulator against data malpractice, victims of ransomware are *victims* of a serious and growing form of transnational crime. In the context of constrained resources, there is, perhaps, a policymaking debate to be had about the balancing act between regulatory due diligence and inadvertently further penalising victims of crime. Ransomware, like other forms of cyber crime, can be a taboo subject matter [64], with victims feeling a sense of shame and embarrassment. If the ICO is perceived to be too inefficient or punitive, this may serve as a disincentive against ransomware victims reporting to the regulator and other authorities. This, in turn, could diminish national data availability regarding the scale, scope and frequency of ransomware.

Limitations and future work

As with all research, there are limitations to the methodology and analysis that should be considered when digesting this work. Qualitative research necessarily relies upon the finding of, and the giving of time from, participants. This may lead to instances where all possible views are not captured, because of the impossibility of interviewing every individual who has experience as, or of helping, ransomware victims. The relative flexibility in the performance of thematic analysis also required the authors to make determinations as to how to engage with the data. The decision to use deductive, latent and constructionist framings necessarily drove analysis that looked to understand perceptions rather than, possibly, the more objective reality of the situation. It is also limited to the experience of individuals with a UK-nexus. However, we consider that the additional reviews provided by the workshop participants at the beginning and end of the process allowed for the creation of additional rigour in our analysis by calling upon a broad range of experts with a wide lived experience who would be able to expose gaps potentially missed by the research team alone.

Additionally, a decision was taken by the authors to limit interviews with victims only to those directly within an organisation impacted by ransomware. Of course, part of the insidious nature of ransomware is the potential for the paralysis of entire organisations, leading to impacts upon service users and clients – and potentially further down the chain still (as noted in [44]). In considering the ability to interview such participants, the authors concluded that the impacts of ransomware as a service user or client may be too difficult to define directly, and thus should be approached in a manner that necessarily would fall out of the scope of this specific research methodology.

More broadly, there are considerable avenues for future research. For instance, as time progresses, there is a growing potential for studies that further our understanding of the long-tail harm(s) of ransomware for both organisation and their employees. The ransomware victims interviewed for this study broadly experienced ransomware incidents across 2020, 2021 and 2022. This has enabled some insight into potential long-tail ransomware harms, but it is apparent that further research could provide more comprehensive insights in this space. One of the most prominent long-tail harms cited by victims was the persistence of ongoing or not-concluded deliberations with the ICO. Policy-focused research could consider whether this is an optimum scenario (i.e., ransomware victims *should* suffer

long-term stress and uncertainty exacerbated by the ICO because they have failed in their duty to protect data) or whether alterations should be made to the status quo (i.e., better resourcing of the ICO in light of the scale of their remit; or a potential re-balancing of data protection regulation vis-à-vis unprovoked cyber breaches).

Additionally, the timeline of ransomware incidents drawn upon for this article overlaps with the SARS-CoV-2 pandemic, which entailed significant disruption (and potential costs or losses) for many organisations. Interviewees cited the challenge of disentangling the full cost of the ransomware incident relative to other disruptors; particularly the pandemic. Whilst the value of a cyber insurance claim (where a cyber insurance policy is present and claimed upon) is an ideal possible indicator of the cost(s) of a ransomware incident, further research could elaborate on the means by which an organisation could measure the financial and non-financial harms experienced during and after the resolution of a ransomware incident.

Conclusion

This work has provided insight into the breadth and depth of harms experienced by ransomware-victim organisations and their staff. Drawing on a large qualitative data corpus that includes the views and experiences of ransomware victims and wider industry stakeholders, including incident responders, ransom negotiators, cyber insurers, law enforcement and government, we have identified that ransomware is a potentially severe organisational risk that can prompt a wide array of significant harms for organisations and their staff. The research corroborates existing reporting [16]; ransomware, through its capacity to cause business interruption and substantial data exposure, can present severe financial and reputational harms to victim organisations. Our exploratory study builds on the existing knowledge base with a wide interview base of professionals and victims who experienced, or worked alongside, ransomware events in the UK, Western Europe and internationally in recent years. This time period coincides with a severe worsening of 'headline' ransomware harms: cost of ransom payment, cost of recovery and timeline of recovery [22, 23]. However, in addition to these headline harms, there is an array of highly significant harms experienced by ransomware victims. This study provides insights into these harms at a critical conjuncture of the growth of ransomware as an organisational and societal threat.

Notably, our study furthers understanding of the significant and under-reported harms that may be experienced by IT and non-IT staff at victim organisations. These harms, which include physiological and psychological harms, can, in some instances, be sufficiently severe to warrant hospitalisation or cause long-term physical or mental health issues. In certain contexts, and particularly for IT staff, there may be a contestation between the incident response (to alleviate organisational harm) and their personal health. The primary concern of an organisation in the midst of a potentially existential ransomware crisis will be the organisational recovery effort. However, as part of its duty-of-care, members of senior management and, where appropriate, the board, should be conscious of the harms that its employees may be experiencing and should undertake efforts to mitigate these during and after the recovery effort. The article has identified a range of measures that can potentially alleviate employee-harms; for instance, the provision of food for those handling the direct incident response and the offering of trauma counselling post-event.

Additionally, organisational *and* staff harms could, possibly, be alleviated (or exacerbated) through a range of factors relating to preparedness, leadership culture and crisis communication. Organisational crisis preparedness plans for other sudden risks (i.e., flood or fire) may not transfer to ransomware. All crises are, arguably, context-dependent and unique, but ransomware was consistently articulated

by interviewees and workshop participants as a unique form of organisational crisis that can place considerable strain on an organisation and its workforce. Additionally, even after an organisation has recovered from a ransomware event, varying forms of harm may be ongoing; for instance, staff PTSD or continuing frustration regarding lost files or new workplace protocols. There is scope for awareness promotion of the breadth and depth of ransomware harms, and measures that may alleviate these harms before, during and after a ransomware event. Existing governmental guidance for organisations – provided through the NCSC's public website and publications – offers apt guidance and correctly identifies ransomware prevention as a board-level responsibility [18, 65], but an elaboration on the scale and severity of harms could help to narrate (a) the unique nature of ransomware risk and (b) the tangible importance of tailored preparedness. This article offers insights that may be useful for such narration.

Ransomware is a dynamic risk, with new threat actors, new attack modalities and new negotiation strategies emerging. In this light, the harm and harm-influence landscape is likely to continue to change over time, with ransomware operators motivated to rationally pursue maximisation of harm(s) in order to leverage greater pressure on victims. This presents an ongoing window for future impactful research on the breadth and depth of ransomware victim harms and the measures that may be undertaken by organisations – and policymakers – to alleviate harms. Mapping the depth and breadth of harms – and the experiencing of harms – is vital in order to ensure that policy measures such as increased sanctions lists [66] or ongoing consideration of a full-ban on ransomware payments [67] can be informed by a comprehensive knowledge of how ransomware impacts organisations, individuals and societies.

Acknowledgements

We would like to thank the participants of this research, particularly the organisations and individuals that have been victims of ransomware attacks. Their openness has been extremely valuable in helping the research community and society in understanding more about the threat and harms of ransomware.

Funding

This work was supported by The Research Institute for Sociotechnical Cyber Security, a collaboration of the UK's Engineering and Physical Sciences Research Council (EPSRC) and the UK's National Cyber Security Centre (NCSC).

References

1. Mott G, Turner S, Nurse J.R.C. et al. Between a rock and a hard(ening) place: cyber insurance in the ransomware era. *Computers and Security* 2023;128.
2. The Gurus. UK second most targeted nation behind America for ransomware. *IT Security Guru* 2023. https://www.itsecurityguru.org/2023/02/07/uk-second-most-targeted-nation-behind-america-for-ransomware (27 July 2023, date last accessed).
3. Tidy J. speaking at RUSI event: The societal impact of ransomware. *Royal United Services Institute*. 2022. https://rusi.org/events/open-to-all/societal-impact-ransomware (27 July 2023, date last accessed).
4. Cabinet Office. National Cyber Strategy 2022. *GOVUK* 2022. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022 (27 July 2023, date last accessed).
5. Collier R. NHS ransomware attack spreads worldwide. *Canadian Medical Association Journal* 2017;189(22).
6. Afifi-Sabet K. Hackney Council services could be offline for 'months' following cyber attack. *IT Pro* 2020. https://www.itpro.com/security/357405/hackney-council-services-disrupted-months-cyber-attack (27 July 2023, date last accessed).
7. Arnold S. Redcar and Cleveland Council ransomware attack could have cost millions. *Northern Echo* 2023. https://www.thenorthernecho.co.uk/news/23293081.redcar-cleveland-council-ransomware-attack-cost-millions/ (27 July 2023, date last accessed).
8. Burt J. Ransomware attack on UK water company clouded by confusion. *The Register* 2022. https://www.theregister.com/2022/08/18/clop_ransomware_uk_water/ (27 July 2023, date last accessed).
9. Morrison S. How a major oil pipeline got held for ransom. *Vox* 2021. https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices (27 July 2023, date last accessed).
10. Marks J. and Shaffer A. Costa Rica shows the damage ransomware can do to a country. *BSA* 2022. https://www.bsa.org/news-events/media/costa-rica-shows-the-damage-ransomware-can-do-to-a-country (11 August 2023, date last accessed).
11. National Security Strategy Joint Committee. Ransomware: call for evidence. *Parliament UK* 2023. https://committees.parliament.uk/work/7017/ransomware/ (27 July 2023, date last accessed).
12. Confederation of British Industry. The 2022 National Cyber Strategy. *CBI* 2022. https://www.cbi.org.uk/articles/the-2022-national-cyber-strategy/ (27 August 2023, date last accessed).
13. Cabinet Office. Government Cyber Security Strategy: 2022 to 2030. *GOVUK* 2022. https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (27 August 2023, date last accessed).
14. Mott G, Nurse J.R.C., Baker-Beall C. Preparing for future cyber crises: lessons from governance of the coronavirus pandemic. *Policy Design and Practice* 2023;6(2)160-181.
15. Institute for Security and Technology. RTF report: combating ransomware. *IST* 2021. https://securityandtechnology.org/ransomwaretaskforce/report/ (27 July 2023, date last accessed).
16. PWC. Cyber security outlook 2023. *PWC* 2023. https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-security-outlook-2023.html (27 August 2023, date last accessed).
17. Microsoft. The growing threat of ransomware. *Microsoft* 2021. https://blogs.microsoft.com/on-the-issues/2021/07/20/the-growing-threat-of-ransomware/ (27 July 2023, date last accessed).
18. NCSC. Ransomware: what you need to know. *NCSC* 2021. https://www.ncsc.gov.uk/files/Ransomware_what_you_need_to_know.pdf (27 July 2023, date last accessed).

19. Janofsky A. Ransomware tracker: the latest figures. *The Record* 2023. https://therecord.media/ransomware-tracker-the-latest-figures (27 July 2023, date last accessed).
20. Dyer J. Ransomware: 2023's top attacks and need-to-know stats. *Egress* 2022. https://www.egress.com/blog/phishing/top-ransomware-attacks-statistics (27 July 2023, date last accessed).
21. Gooding M. UK regulators warn lawyers to stop making ransomware payments for clients. *Tech Monitor* 2022. https://techmonitor.ai/technology/cybersecurity/ransomware-payments-uk-lawyers-ico-ncsc (27 July 2023, date last accessed).
22. Sophos. The state of ransomware 2022. *Sophos* 2022. https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/ (27 July 2023, date last accessed).
23. Sophos. The state of ransomware 2023. *Sophos* 2023. https://www.sophos.com/en-us/whitepaper/state-of-ransomware (27 July, 2023, date last accessed).
24. CISA. Cost of a cyber incident: systematic review and cross-validation. *CISA* 2020. https://www.cisa.gov/resources-tools/resources/cost-cyber-incident-systematic-review-and-cross-validation (11 August 2023, date last accessed).
25. Connolly L, Wall D, Lang M. et al. An empirical study of ransomware attacks on organisations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* 2020;6(1)1-18.
26. DCMS. Exploring organisational experiences of cyber security breaches. *GOVUK* 2022. https://www.gov.uk/government/publications/exploring-organisational-experiences-of-cyber-security-breaches (27 July, date last accessed).
27. Heyburn H, Whitehead A, Zanobetti L. et al. Analysis of the full costs of cyber security breaches. *Ipsos Mori* 2020. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf (27 July 2023, date last accessed).
28. Zhang-Kennedy L, Assal H, Rocheleau J. et al. The aftermath of a crypto-ransomware attack at a large academic institution. *Proceedings of the 27th USENIX Security Symposium*. 2018, 1061-1078.
29. Harvey H, Amberger-Murphy, V, Ballot, J. et al. Impact of Conti ransomware attack on cancer trials Ireland sites. *Journal of Clinical Oncology* 2022;40.
30. Zhao J, Kessler E, Yu J. et al. Impact of trauma hospital ransomware attack on surgical residency training. *Journal of Surgical Research* 2018;232:389-397.
31. CISA. Understanding ransomware threat actors: LockBit. *CISA* 2023. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (27 July 2023, date last accessed).
32. Cleary Q. The devastating impact of ransomware attacks on small businesses. *University of Maryland Francis King Carey School of Law* 2023. https://www.law.umaryland.edu/content/articles/name-659577-en.html (27 July 2023, date last accessed).
33. Simoiu C, Symanetic C, Bonneau J. et al. 'I was told to buy a software or lose my computer. I ignored it': a study of ransomware. *Proceedings of the Fifteenth Symposium on Usable Privacy and Security* 2019, 155-174.
34. Ortloff A, Vossen M, Tiefenau C. Replicating a study of ransomware in Germany. *European Symposium on Usable Security* 2021, 151-164.
35. Button M, Blackbourn D, Sugiura L. et al. From feeling like a rape to a minor inconvenience: victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics* 2021;64.
36. Lang M, Connolly L, Taylor P. et al. The evolving menace of ransomware: a comparative analysis of pre-pandemic and mid-pandemic attacks. *Digital Threats: Research and Practice* 2022.

37. Mujaye S. Ransomware: to pay or not to pay? The results of what IT professionals recommend. *Proceedings of the 5th International Conference on Software Engineering and Information Management* 2022, 76-81.
38. Connolly A, Borrion H. Reducing ransomware crime: analysis of victims' payment decisions. *Computers and Security* 2022;119.
39. Connolly A, Wall D. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomizing countermeasures. *Computers and Security* 2019;87.
40. Haner M, Sloan M, Graham, A. et al. Ransomware and the Robin Hood effect? Experimental evidence on Americans' willingness to support cyber-extortion. *Journal of Experimental Criminology* 2022.
41. Shandler R, Gomez M. The hidden threat of cyber-attacks – undermining public confidence in government. *Journal of Information Technology and Politics* 2022.
42. Caroscio E, Paul J, Murray J. et al. Analysing the ransomware attack on D.C. Metropolitan Police Department by Babuk. *Proceedings of the 16th Annual IEEE International Systems Conference* 2022.
43. Jarjoui S, Murimi R, Murimi R. Hold my beer: a case study of how ransomware affected an Australian beverage company. *Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment* 2021.
44. Pattnaik N, Nurse JRC, Turner S. et al. It's more than just money: the real-world harms from ransomware attacks. *17th International Symposium on Human Aspects of Information Security and Assurance* 2023.
45. Braun V, Clarke, V. Using thematic analysis in psychology. *Qualitative Research in Psychology* 2006;2:77-101.
46. Hadan H, Serrano N, Camp L. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. *Journal of Cybersecurity* 2022;7.
47. Bryman, A. Social research methods. Oxford University Press, London. 2016.
48. Agrafiotis I, Nurse J.R.C., Goldsmith M. et al. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate, *Journal of Cybersecurity* 2018;4.
49. Ton J. Ransomware damage: are you forgetting about your reputation? *Forbes* 2022. https://www.forbes.com/sites/forbestechcouncil/2022/04/08/ransomware-damage-are-you-forgetting-about-your-reputation/?sh=228c4d4c5c48 (27 July 2023, date last accessed).
50. Aon. Reputational damage and cyber risk go hand in hand. *Aon* 2019. https://www.aon.com/unitedkingdom/insights/reputational-damage-and-cyber-risk.jsp (27 July 2023, date last accessed).
51. Tidy J. How a ransomware attack cost one firm £45m. *BBC* 2019. https://www.bbc.co.uk/news/business-48661152 (27 July 2023, date last accessed).
52. Whitney L. The many ways a ransomware attack can hurt your organisation. *Tech Republic* 2021. https://www.techrepublic.com/article/the-many-ways-a-ransomware-attack-can-hurt-your-organization/ (27 July 2023, date last accessed).
53. O'Gara C. Ransomware attacks causing employee layoffs. *Secure World* 2020. https://www.secureworld.io/industry-news/ransomware-attacks-causing-employee-layoffs (27 July 2023, date last accessed).
54. Sharton B. Ransomware attacks are spiking. Is your company prepared? *Harvard Business Review* 2021. https://hbr.org/2021/05/ransomware-attacks-are-spiking-is-your-company-prepared (27 July 2023, date last accessed).
55. Spiewak R, Renyolds T, Weitzner D. Ransomware readiness index: a proposal to measure current preparedness and progress over time. *Internet Policy Research Initiative* 2021. https://dspace.mit.edu/bitstream/handle/1721.1/132615/Spiewak-Reynolds-Weitzner-RansomwareReadinessIndex-IPRI-2021-WP-02.pdf?sequence=1&isAllowed=y (27 July 2023, date last accessed).

56. Haggman A. Cyber wargaming: finding, designing, and playing wargames for cyber security education. *Royal Holloway* 2019. https://pure.royalholloway.ac.uk/ws/portalfiles/portal/33911603/2019haggmanaphd.pdf (27 July 2023, date last accessed).
57. Stevens A. Ransomware recovery – 5 action items missing from your plan. *Versprite* 2023. https://versprite.com/blog/5-action-items-missing-from-your-ransomware-recovery-plan/ (27 July 2023, date last accessed).
58. Baker T, Shortland A. Insurance and enterprise: cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance – Issues and Practice* 2023;48:275-299.
59. Ahmad T. Coronavirus pandemic and work from home: challenges of cybercrimes and cybersecurity. *SSRN* 2020.
60. Pranggono B, Arabo A. Covid-19 pandemic cybersecurity issues. *Internet Technology Letters* 2020.
61. Woods D, Bohme R. How cyber insurance shapes incident response: a mixed methods study. *The 20th Workshop of the Economics of Information Security* 2021.
62. NCSC. CIR – Cyber incident response. *NCSC* 2023. https://www.ncsc.gov.uk/information/cir-cyber-incident-response (27 July 2023, date last accessed).
63. Afifi-Sabet K. Brave accuses the ICO of 'falling asleep at the wheel'. *IT Pro* 2020. https://www.itpro.com/policy-legislation/data-protection/356423/ico-lambasted-for-falling-asleep-at-the-wheel (27 July 2023, date last accessed).
64. Schwartz S. The forgotten ones: ransomware preys on the resource-poor. *CIO Dive* 2019. https://www.ciodive.com/news/the-forgotten-ones-ransomware-preys-on-the-resource-poor/565062/ (27 July 2023, date last accessed).
65. NCSC. Cyber security toolkit for boards. *NCSC* 2022. https://www.ncsc.gov.uk/files/NCSC_Cyber-Security-Board-Toolkit.pdf (27 July 2023, date last accessed).
66. NCA. Ransomware criminals sanctioned in joint UK/US crackdown on international cyber crime. *NCA* 2023. https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime (27 July 2023, date last accessed).
67. Fung B, Sands G. FBI tells Congress ransomware payments shouldn't be banned. *CNN* 2021. https://edition.cnn.com/2021/07/27/politics/senate-judiciary-ransomware-hearing/index.html (27 August 2023, date last accessed).
68. Ell M, Rizvi S. Cyber security breaches survey 2024. *DSIT*. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 (22 May 2024, date last accessed).
69. Biggs A, Brough P, Barbour, J. Exposure to extraorganisational stressors: impact on mental health and organisational perceptions for police officers. *International Journal of Stress Management* 2014; 21.
70. Talas R, Button M, Doyle M, et al. Violence, abuse and the implications for mental health and wellbeing of security operatives in the United Kingdom: the invisible problem. *Policing and Society* 2021; 31.
71. Fichera G, Fattori L, Neri M, et al. Post-traumatic stress disorder among bank employee victims of robbery. *Occupational Medicine* 2015;65.
72. Wesemann U, Applewhite B, Himmerich H. Investigating the impact of terrorist attacks on the mental health of emergency responders: systematic review. *BJPsych Open* 2022;8.
73. Parkin, S., Kuhn, K., Shaikh, S.A. Executive decision-makers: a scenario-based approach to assessing organizational cyber-risk perception, *Journal of Cybersecurity*, 2023:9-1.

Appendix A: Interview questions

Questions for victim organisations

Overview

What is your role?

How many years of experience do you have in your industry?

What is the size of your organisation (in terms of employees and turnover)?

Impact and harms

Has your organisation been the victim of a ransomware incident in the past? If so, can you tell us more about it and what happened to your IT systems/data etc.

What were the negative impacts of the attack on your organisation? E.g. financial, reputational

Did the attack have any negative impacts on your customers/suppliers/clients etc.?

What was the impact of the attack on your employees? What was the impact on you as an individual?

If we think about the harms of a ransomware attack on a timeline, for instance, immediate (within hours or days), short term (within weeks), medium term (6-12 months), and long term (12+ months), where would you place each of the various harms that you mentioned?

Are there any negative impacts or harms that are often overlooked or forgotten about, but that may be regarded as particularly important?

Did you try and measure or quantify the impact of the attack on your organisation? If not, did you try and document the impact of the attack on your organisation in any way?

The victim experience

Which third-parties supported you (e.g. incident response, insurer, lawyers, law enforcement, NCSC)? And which services were helpful?

What factors aggravate the negative experience encountered by a victim organisation after a ransomware incident?

What factors reduce the negative experience encountered by a victim organisation after a ransomware incident?

Did you report the incident to the NCSC, law enforcement, Action Fraud or a regulator? Did you find the process easy to navigate?

What factors during the victim's experience encourage or discourage the likelihood of reporting ransomware to law enforcement, regulators or relevant government agencies?

Do you think there is sufficient government or law enforcement support for victims of ransomware? What kind of additional support would have helped?

Did you tell the public, clients, customers etc. that you'd been hit by ransomware? What influenced your communications strategy?

In hindsight, would you have managed the incident differently?

Questions for practitioners/law enforcement

Overview

What is your role?

How many years of experience do you have in your industry?

What is the size of your organisation (in terms of employees and turnover)?

Impact and harms

In your role, have you engaged with organisations who have been the victim of ransomware attacks in the past? If so, are there any that stand out and can you tell us what happened?

Can you explain or list the variety of harms that you think can result, including non-financial impacts (i.e. psychological, reputational etc) on victims? Is harm greater for data exfiltration?

If we think about the harms of a ransomware attack on a timeline, for instance, immediate (within hours or days), short term (within weeks), medium term (6-12 months), and long term (12+ months), where would you place each of the various harms that you mentioned?

What are some of the downstream or second-order harms of ransomware? E.g. for individuals, society or national security?

Are there any harms that are often overlooked or forgotten about, but that may be regarded as particularly important?

Which harms do you think you have the most and least visibility into?

How typical is it for victims to conduct after-action reviews?

The victim experience

Based on your experience, can you talk us through your role as a third-party supporting the victim? What sort of services do you provide to support victims of ransomware?

How long does your engagement with victims typically last for?

What factors aggravate the negative experience encountered by a victim organisation after a ransomware incident?

What factors reduce the negative experience encountered by a victim organisation after a ransomware incident?

How typical is it for victims to report a ransomware attack to the NCSC, law enforcement, Action Fraud or a regulator? What is your role in the notification process? Is the notification process easy to navigate?

What factors during the victim's experience encourage or discourage the likelihood of reporting ransomware to law enforcement, regulators or relevant government agencies?

Do you think there is sufficient government or law enforcement support for victims of ransomware? What should be done to improve support for victims?

In your experience, what influences victims' approach to comms following a ransomware attack?

Law enforcement specific questions

Does your cybercrime unit work with any specific type of victim or investigate any specific strains of ransomware?

What is the process for triaging victims that report to law enforcement? What percentage of victims typically receive incident management support from the NCA or a ROCU?

What – if anything – would you change about the current law enforcement approach to supporting victims? What sources of resources or capabilities do you need to support your work?

<u>Questions for government (and policymakers)</u>

Overview

What is your role?

How many years of experience do you have in government?

How critical is the ransomware threat today? Do you see this threat increasing in the future?

Impact and harms

In your role, have you engaged with organisations who have been the victim of ransomware attacks in the past? If so, are there any that stand out and can you tell us what happened?

We're especially interested in the harms (negative impacts) that can result from ransomware attacks. Can you explain or list the variety of harms that you think can result?

If we think about the harms of a ransomware attack on a timeline, for instance, immediate (within hours or days), short term (within weeks), medium term (6-12 months), and long term (12+ months), where would you place each of the various harms that you mentioned?

Are there any harms that are often overlooked or forgotten about, but that may be regarded as particularly important?

Which harms do you think government has the most and least visibility into?

The victim experience

What factors aggravate the negative experience encountered by a victim organisation after a ransomware incident?

What factors reduce the negative experience encountered by a victim organisation after a ransomware incident?

What types of government support are there for victims of ransomware?

Are there any policy changes on the horizon that might give victims access to other types of support, or change the type of support they currently receive?

How typical is it for victims to report a ransomware attack to the NCSC, law enforcement, Action Fraud or a regulator (e.g. the ICO)? Is the notification process sufficiently easy to navigate?

What factors during the victim's experience encourage or discourage the likelihood of reporting ransomware to law enforcement, regulators or relevant government agencies?

Do you think there is sufficient government support for victims of ransomware? What should be done to improve support for victims?

Appendix B: Code book

Table 7: Code book

High-level code	Sub-codes
Harms from attack	Financial Non-financial
Negative Impacts	On direct customers or clients On IT employees On non-IT employees On organisation On others
Reflections on the attack	Preparedness vs reality What makes managing it go well What makes managing it go worse What would do differently
Reporting and Comms	Business partners, supply chains etc To employees and customers To regulators and government To the public With attackers With other victims
Role of the government and law enforcement	Clarity around which govt or LE agency does what Improvement suggestions They do not help enough They help enough
Timeline of harms	Immediate Long-term (years) Medium-term (months) Short-term (weeks)
Victim experience	Emotions mentioned Exfiltration vs encryption Handling the recovery effort How do third parties help How do third parties hinder Post event audit Ransom paid vs not paid