RUSI

University of Kent

supported by National Cyber Security Centre

RISCS Research Institute for Sociotechnical Cyber Security

Occasional Paper

‘Your Data is Stolen and Encrypted’: The Ransomware Victim Experience

Pia Hüsch, Gareth Mott and Jamie MacColl, with Jason R C Nurse, James Sullivan, Sarah Turner and Nandita Pattnaik

Occasional Paper

193 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 193 years.

Published in 2024 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, July 2024. ISSN 2397-0286 (Online).

Cover image: James Thew / Alamy Stock Photo

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

Contents

Executive Summary

More individuals and organisations in the UK and globally are becoming victims of ransomware. However, little is known about their experiences. This paper sheds light on the victim experience and identifies several key factors that typically shape such experiences.

These factors are context-specific and can either improve or worsen the victim experience. They include the following:

- **Timing of an incident**, which may happen after a victim has increased their cyber security measures or at an already stressful time for an organisation, such as the beginning of a school year.
- **Level of preparation** in the form of strong cyber security measures and contingency plans explicitly tailored to respond to a cyber incident.
- **Human factors**, such as the workplace environment and pre-existing dynamics which are often reinforced during an incident. Good levels of unity can bring staff together during a moment of crisis, but a lack of leadership or a blame culture are likely to aggravate the harm experienced during the incident.
- **Engagement with third-party service providers**, such as those providing technical incident response or legal services, can alleviate the negative aspects of the victim experience by providing critical legal, technical or other help. However, they may aggravate the harm by providing poor services or losing valuable time in responding to the incident.
- A successful **communications campaign** is highly context and victim specific. It must include external and internal communications with staff members not part of the immediate response to ensure a good workplace culture.

For support, many victims turn to public sector institutions such as law enforcement. Expectations for technical support and expertise from law enforcement are generally low, but victims feel especially unsupported where phone calls are not returned and there is no engagement or feedback loop. The National Cyber Security Centre enjoys a better reputation. However, there is widespread uncertainty about its role and the thresholds that must be met for it to provide support. This poses a reputational risk.

Understanding how ransomware attacks are personally felt by victims and what factors aggravate or alleviate the harm they experience is key for policymakers seeking to implement measures to minimise harm as much as possible.

Summary of Recommendations

- While ransomware causes many kinds of harm, mitigating the psychological impact of ransomware attacks needs to be at the centre of the support given to (potential) victims preparing for and responding to a ransomware incident.
  - Third-party service providers also need to recognise that efforts mitigating the psychological impact of ransomware attacks are critical to improving victims' experience. They must therefore form part of their technical, legal or other services.
  - Public policy on ransomware must centre on measures that mitigate victims' harm. This includes acknowledging and mitigating the psychological impact on victims, for example through counselling, compensation or time off in lieu.
- Victims should aim for the right balance of discretion and transparency within their external and internal communications.
- Third-party service providers should actively enable information sharing, subject to the consent of parties, among past, current and potential victims through their networks.
- Law enforcement and intelligence agencies should establish a positive feedback loop that shares success stories and notifies victims when the information they share has been successfully used for intelligence and law enforcement activities.
- Government authorities need to clarify the tasks of relevant public institutions and their role in the ransomware response, including who can receive support and under what circumstances.
- Given year-on-year increases in the frequency of incidents, the resourcing of the Information Commissioner's Office should be routinely assessed to enable timely assessments of ransomware breaches.

Introduction

When staff at Hackney Council encountered outages of its IT systems in October 2020, it quickly became evident that the council was facing a cyber attack. But the employees did not know that they would be dealing with its effects for years.[1] Those who experience a ransomware attack experience a crisis, possibly even an existential threat for an attacked organisation and its staff. For those involved, it represents a low point in their professional and possibly even private lives, with consequences that are felt far beyond the immediate response.[2]

At Hackney Council, staff members had to improvise while their access to data and technology was disrupted, working long hours to compensate for the technical problems. Meanwhile, more than 250,000 residents living in the borough faced disruptions and delays to critical council services, including housing benefits, social care, council tax and business rates. Years after the incident, the repercussions were still being felt.[3] These insights are based on unusually detailed public reporting of the aftermath of Hackney Council's ransomware incident. However, they still provide few details on the actual victim experience.

The staff and residents of Hackney Council are, of course, not the only ones affected by ransomware attacks. Ransomware criminals continue to target businesses of all sizes, as well as schools, healthcare providers, universities, charities and government entities. Prominent examples of 2023 ransomware victims in the UK include Royal Mail, an NHS trust and the outsourcing firm Capita, which handles the British Army's recruitment process.[4]

Since the mid-2010s, ransomware has emerged as one of the most harmful forms of cyber-criminal activity for organisations. Ransomware operators encrypt files or systems, demanding a ransom payment in return for a private key to decrypt the affected data. Increasingly, ransomware operators also exfiltrate victims' data and threaten to leak it on the darknet unless a ransom is paid. For an organisation and its employees this can be an extremely stressful, high-pressure incident that causes a wide range of harm to individuals, organisations and society at large.[5]

1. Matt Burgess, 'The Untold Story of a Crippling Ransomware Attack', *Wired*, 30 January 2023.
2. Jamie MacColl et al., 'The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society', *RUSI Occasional Papers* (January 2024).
3. Burgess, 'The Untold Story of a Crippling Ransomware Attack'.
4. Dan Milmo, 'Who is Behind the Latest Wave of UK Ransomware Attacks?', *The Guardian*, 14 September 2023.
5. Examples from the same dataset are analysed in the first paper of RUSI's project 'Ransomware Harms and the Victim Experience', which also provides a framework for different types of harm. See MacColl et al., 'The Scourge of Ransomware'.

Although more individuals and organisations are becoming victims of ransomware attacks, little is known about the victim experience. Reporting often focuses on financial implications or technical details. In contrast, this paper sheds light on how organisations and their staff experience a ransomware attack. It offers a particular focus on the specific factors that – for better or worse – influence this experience. These factors include: the scale and timing of the incident; the size of the victim organisation; the level of preparation undertaken by the victim organisation prior to the ransomware event; the nature of the existing workplace culture; and the experience of dealing with third parties that form part of the ransomware response ecosystem, including the UK National Cyber Security Centre (NCSC) and law enforcement; the role of communication; and the role of transparency and information sharing.

Offering such detailed insights into the victims' experiences of a ransomware attack gives policymakers, cyber security professionals and practitioners in the ransomware response ecosystem key knowledge. This is pivotal when designing effective response plans and policy measures and conducting incident response. It is also essential for providing personalised support to any victims. The research findings for this paper also inform any organisation or individual preparing for a possible ransomware attack or other cyber incident of what challenges they might face and how they can prepare for them.

Structure

This paper is structured as follows. Chapter I draws findings from, and identifies research gaps in, existing research, reporting and data that build an understanding of the victim experience. Chapter II summarises the findings from the original research to identify the factors that influence the ransomware victim experience, including: the scale and timing of the incident; the size of the victim organisation; the level of preparation undertaken by the victim organisation prior to the ransomware event; the nature of the existing workplace culture; and the experience of dealing with third parties that form part of the ransomware response ecosystem. The third-party organisations included in the analysis are those that were seen as most significant by interviewees and workshop participants. These are lawyers, insurance providers, incident responders, ransom negotiators and public relations firms. Chapter III analyses the role of public sector bodies, including local and regional police, the NCSC, the National Crime Agency (NCA) and the Information Commissioner's Office (ICO). The paper concludes with a range of policy recommendations.

Methodology

This paper is part of a series of research publications resulting from a 12-month research project, 'Ransomware Harms and the Victim Experience', conducted by RUSI and the University of Kent.[6] The project is funded by the UK's NCSC and the Research Institute for Sociotechnical Cyber Security. Its aim is to understand the wide range of harm caused by ransomware attacks to individuals, organisations and society at large.

The research project focuses on the question: How is a ransomware attack experienced by victims, and what factors aggravate or reduce the negative experience(s)?

The data collection and analysis for this paper entailed a literature review, semi-structured interviews and workshops.

Literature Review

The project started with a literature review of publicly available sources on ransomware harm and ransomware victims. It included a non-systematic review of publicly available academic and grey literature, including surveys and reports produced by stakeholders of the ransomware ecosystem. The initial literature review was conducted in August and September 2022.

Semi-Structured Interviews

The primary dataset for the paper is based on 42 semi-structured online interviews with both victims of ransomware attacks and subject-matter experts from across the ransomware ecosystem, including individuals from the insurance industry, government, law enforcement and incident responders. An overview of the background of interviewees is provided in Tables 1 and 2.

Interviewees from ransomware victim organisations included both IT and non-IT staff. The scope of the interviews included personnel at a ransomed organisation; the research team did not interview wider knock-on victims (for example, those in supply chains or clients). Non-victim interviewees were selected for their breadth and depth of experience that involved multiple ransomware incidents spanning several years. Interviewees were predominantly from the UK, although a limited number were based in the US or other countries in Western Europe. Interviews were conducted between November 2022 and March 2023.

6. RUSI, 'Ransomware Harms and the Victim Experience', <https://rusi.org/explore-our-research/projects/ransomware-harms-and-victim-experience>, accessed 14 June 2024.

All interview data was anonymised to allow individuals to speak openly about potentially sensitive issues. The research team then analysed the interview transcripts using a thematic analysis approach, which involved generating codes that reoccurred in interviews and identifying themes that provided insight into the research questions. The analysis was conducted using NVIVO. An anonymised coding system based on Tables 1 and 2 is used to refer to interview data in the footnotes.

Table 1: Breakdown of Non-Victim Interviewees

Type of Organisation	Number of Participants
Digital forensics and incident response	7
Ransomware specialist	3
External counsel	4
Insurance claims	3
Crisis communications	1
NCSC	2
Law enforcement	2
Total	**22**

Source: The authors.

Table 2: Breakdown of Victim Interviewees

Type of Organisation	Number of Participants
Education	4
Engineering	1
Consultancy	2
Financial services	1
Foreign government	1
Government agency	2
Charity	1
Local government	2
Manufacturer	1
Professional services	1
Technology	3
Outsourcing	1
Total	**20**

Source: The authors.

Workshops

The research team conducted two online workshops with key stakeholders from the UK government, the insurance and cyber security industries, lawyers and law enforcement. They were held in November 2022 and February 2023. Attendees included a mix of interviewees and new participants, using contacts established during the interview phase. The first workshop was used for data gathering. The second workshop was used to validate the research findings.

Limitations

This research project has been based on a large data corpus, drawing on interviews with ransomware victims and stakeholders from the ecosystem who support ransomware victims. Data collection therefore relied on the voluntary participation of ransomware victims and their support ecosystem. Understandably, victims of ransomware are often hesitant or unwilling to speak of their experience. The authors note the possibility of some participatory selection bias; for instance, ransomware victim interviewees who were willing to voluntarily give up their time to speak to the research team may also have been more likely to reach out to law enforcement or report to the ICO. It is also possible that ransomware victims who were willing to describe their experiences in a voluntary research setting may also have been less likely to have paid a negotiated ransom. Additionally, the majority of interviewees were UK-based; it is possible that geographic and, especially, cultural contexts affect ransomware experiences. The findings from this research therefore cannot be said to represent a universal ransomware experience.

It is important to note that the findings of this project provide insights from a 'snapshot' of the ransomware victim experience across a particular timeframe, with interviews ending in March 2023. As highlighted from this project's data corpus, ransomware victims' experiences are not the same; there is substantial variability that depends on internal and external factors. As ransomware is a dynamic threat that continues to evolve, it is important that researchers continue to engage with victims of ransomware to further build the understanding of how the experiences of future victims can be improved.

I. Existing Insights on the Ransomware Victim Experience

Each ransomware incident is unique, although collectively ransomware experiences have much in common. A ransomware attack will typically follow a set of stages involving an initial attempt to access an IT estate, a successful breach, followed by further access across the network. The attackers will then seek to gain greater privileges, identify their desired sections of the network, exfiltrate data (if they are exfiltrating) and deliver their encryption payload (if they are encrypting). The attackers will then typically either use a splash screen or otherwise make contact with the victim to encourage them to commence discussions about ransom payment.[7] As a general timeline, once a ransomware victim notices that they have been breached and/or have been contacted by the ransomware operators, there generally follows an immediate crisis period – which could last days or weeks – during which they seek to contain the attackers' access, restore core systems and assess what data may have been exfiltrated. During this time, the organisation may or may not be able to operate normal functions. This core crisis period is followed by a gradual or staggered transition to normal operations. Victims of ransomware will often draw on the support of a range of third-party services, including but not limited to: cyber insurers; incident responders; ransom negotiators; lawyers; public relations services; and law enforcement or national cyber authorities (such as the NCSC in the UK). The roles that these services can play in influencing the ransomware victim's experiences are explored later in this paper.

Some understanding of 'typical' ransomware victim experiences can be acquired through news reports and existing analyses of mostly objective factors, such as the financial and temporal impact of an attack. A novel study by Nandita Pattnaik and others drew on public reporting relating to a range of ransomware incidents to identify the scale and depth of harms to the victim organisation(s).[8] More

7. Nathan Cross, 'Timeline of a Typical Ransomware Attack', *Medium*, 26 October 2022; National Cyber Security Centre (NCSC), 'Incident Management: Appendix: Incident Timelines', 19 September 2019, <https://www.ncsc.gov.uk/collection/incident-management/appendix-incident-timelines>, accessed 10 June 2024.
8. Nandita Pattnaik et al., 'It's More Than Just Money: The Real-World Harms from Ransomware Attacks', in Steven Furnell and Nathan Clarke (eds), Proceedings of International Symposium on Human Aspects of Information Security and Assurance, Kent, 4–6 July 2023, pp. 261–74.

broadly, media attention focuses on the scale and scope of contemporary criminal ransomware activity, and the significant disruption that can be caused to organisations. An example of a widely reported ransomware incident is the DarkSide attack against Colonial Pipeline, a US gas supplier, in May 2021.[9] As a result of the incident, the company switched off its pipeline systems for six daysand reportedly paid the attackers $4.4 million.[10] Other attacks may be more prolonged. In October 2020 in the UK, Hackney Council was attacked by the Pysa ransomware group, which encrypted systems and exfiltrated sensitive data. A range of the council's services, including critical services such as housing benefit and social care services, were not fully operable for roughly a year.[11] In October 2022, it was reported that the cost of Hackney Council's recovery effort in the prior financial year exceeded £12 million.[12]

Reports on ransomware attacks often depend on the information released either by a victim organisation or their legal representatives, or possibly the attackers themselves. For example, in January 2022 the British convenience food manufacturer, KP Snacks, was attacked by the Conti ransomware group. The attack became publicly known on 2 February, after the firm sent a letter to its distributors notifying them of a cyber attack.[13] The Conti group darknet leak page shared examples of sensitive employee data – including birth certificates and credit card statements – and the group allegedly gave KP Snacks five days to pay a demanded ransom to prevent more proprietary data from being leaked.[14] It is not clear what was the value of the ransom, whether it was paid, and how prolonged the impact within the company was. In such instances, insights into the victim experience are highly limited.

Other reports have assessed a range of ransomware attacks in aggregation to quantify average ransomware impacts. Expense and downtime can be used as broad measures of victim harms and/or experience. For example, the most recent annual Sophos State of Ransomware report identified that the average ransom payment had reached more than $1.5 million (the median was $400,000).[15]

9. Sean Michael Kerner, 'Colonial Pipeline Hack Explained: Everything You Need to Know', TechTarget, 26 April 2022, <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know>, accessed 24 June 2024.
10. *BBC News*, 'Colonial Pipeline Boss Confirms $4.4m Ransom Payment', 19 May 2021.
11. Burgess, 'The Untold Story of a Crippling Ransomware Attack'.
12. Julia Gregory, 'Cyber Attack Recovery Effort Cost Hackney Council over £12m Last Year', *Hackney Citizen*, 13 October 2022, <https://www.hackneycitizen.co.uk/2022/10/13/cyber-attack-recovery-hackney-council-12m/>, accessed 10 June 2024.
13. Ax Sharma, 'KP Snacks Giant Hit by Conti Ransomware, Deliveries Disrupted', *Bleeping Computer*, 2 February 2022, <https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliveries-disrupted/>, accessed 14 June 2024.
14. Brenda Robb, 'The State of Ransomware in 2022', BlackFog, 4 January 2023, <https://www.blackfog.com/the-state-of-ransomware-in-2022/#>, accessed 24 June 2024.
15. Sophos, 'The State of Ransomware 2023', Sophos Whitepaper, May 2023, <https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf>, accessed 10 June 2024.

Ninety-seven percent of victims were reportedly able to regain access to their data, with backups the most common recovery method (70%), while 46% of victims elected to pay the ransom for a decryption key.[16] The average overall recovery cost for victim organisations was reported to be $1.82 million.[17] Drawing on Kovrr's cyber incident database, a 2022 report by Check Point Research identified that the average 'attack duration' was 9.9 days in 2021.[18] However, while providing valuable information, these statistics reduce the victim to an abstract number and statistical event and do not account for the deeply personal experience a victim goes through when their organisation has been affected by a ransomware incident.

To provide further insights into the victim experience beyond these initial metrics, academics and researchers conducted surveys and interviews with ransomware victims. This approach can enable more in-depth understanding and analysis of a given ransomware event. The ethical frameworks governing academic research may also provide assurances to ransomware victims, for example regarding anonymisation and data handling, which give the victims confidence to speak. This could include research into events that are not reported in-depth publicly. Leah Zhang-Kennedy and others focused on a ransomware incident at a US university, surveying 150 students and faculty members and interviewing 30 individuals to gain a range of perspectives about a single incident.[19] Harry Harvey and others and Jane Y Zhao and others have conducted studies that have drawn insights from interviews with medical staff at healthcare organisations subject to ransomware, identifying the impact the incidents had on colleagues' provision of care, and their emotional toll.[20] A 2020 study by Lena Yuryna Connolly and others drew on original interviews with IT and security managers from 10 organisations to identify attack characteristics including ransom value and the nature of lost data.[21] A study by the UK's Department for Digital, Culture, Media & Sport drew on interviews involving 10 victim organisations that had experienced a range of ransomware or non-ransomware

16. *Ibid.*
17. *Ibid.*
18. Kovrr specialises in the quantification of cyber risks. See Check Point Research, 'Behind the Curtains of the Ransomware Economy – The Victims and the Cybercriminals', 28 April 2022, <https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/>, accessed 17 June 2024. The report defines the attack duration as the time between the start of the ransomware attack and the resumption of normal operations at the victim organisation.
19. Leah Zhang-Kennedy et al., 'The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution', presentation to the Proceedings of the 27th USENIX Security Symposium, Baltimore, MD, 2018.
20. Harry Harvey et al., 'The Impact of a National Cyberattack Affecting Clinical Trials: The Cancer Trials Ireland Experience', *JCO Clinical Cancer Informatics* (Vol. 7, 2022); Jane Y Zhao et al., 'Impact of Trauma Hospital Ransomware Attack on Surgical Residency Training', *Journal of Surgical Research* (Vol. 232, December 2018), pp. 389–97.
21. Lena Yuryna Connolly et al., 'An Empirical Study of Ransomware Attacks on Organisations: An Assessment of Severity and Salient Factors Affecting Vulnerability', *Journal of Cybersecurity* (Vol. 6, No. 1, 2020), pp. 1–18.

cyber breaches – with two employees from each – to develop case studies, exploring each organisation's context and the impact of their cyber breach.[22]

As a rule of thumb, wider news reporting and annual summaries of ransomware attacks primarily focus on financial impacts or offer technical insights on how they were conducted. These are invaluable as a means of providing insight into the occurrence of ransomware and general trends and it is vital that journalists, private companies, governments and NGOs continue to publish frequently. However, the experiences of the individuals in the midst of the event are rarely discussed in reports and summaries. The interview-based research for this paper is an approach that can bring individuals and their experiences to the fore. Ransomware is a dynamic threat that has continued to change over time with, for example, new attack modalities, the emergence of ransomware-as-a-service and altered negotiation strategies. As such, academics, the wider public and policymakers must conduct further research to develop an understanding of the multi-faceted immediate, mid-term and long-term ransomware victim experience.

22. Ipsos, 'Exploring Organisational Experiences of Cyber Security Breaches', 2021, <https://www.gov.uk/government/publications/exploring-organisational-experiences-of-cyber-security-breaches>, accessed 10 June 2024.

II. Factors Affecting the Victim Experience

Gaining new understanding of what it is like to experience a ransomware incident helps policymakers to design policy interventions. Such interventions can explicitly consider evidence that demonstrates where harm occurs as well as what can alleviate the negative aspects of such experiences. Understanding the victim experience is an essential requirement to design effective policy interventions that counter victims' harm. This chapter illustrates what victims experience and what factors alleviate or elevate the harm caused.

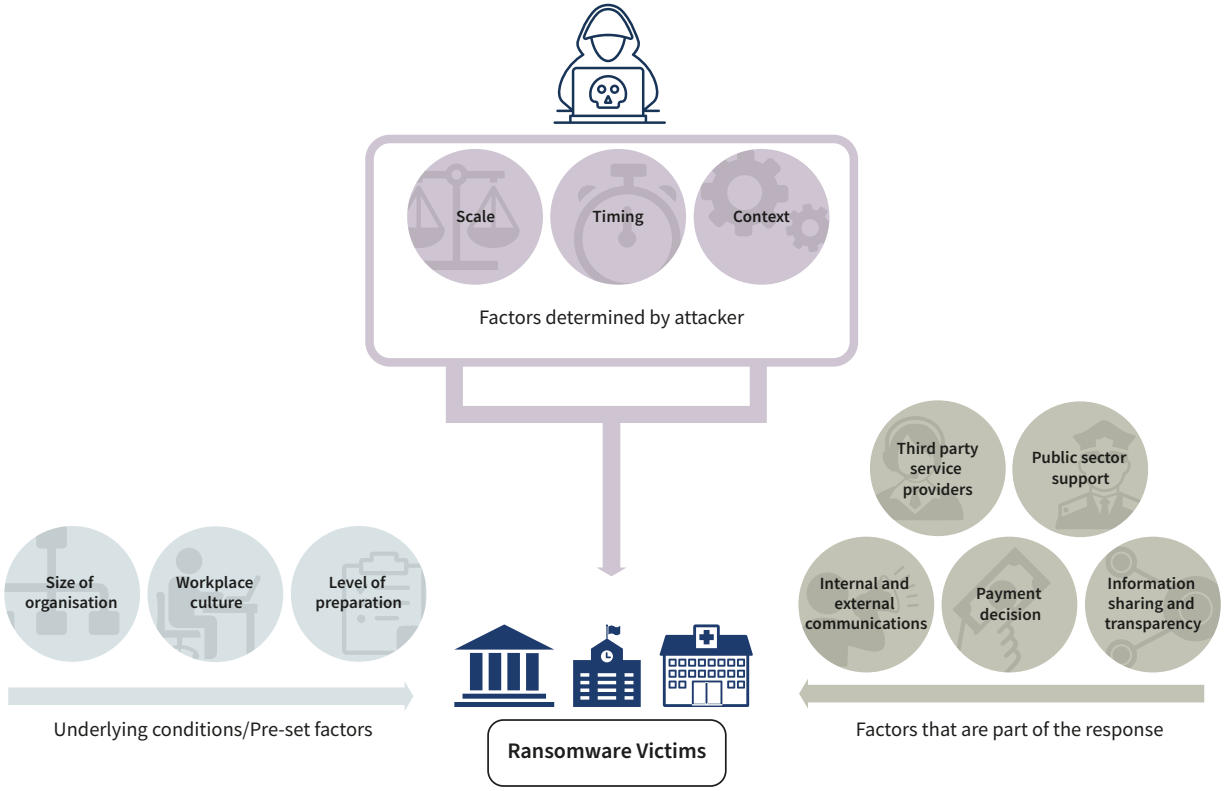
The paper is structured around several key themes that impact the victim experience and that were identified based on the interview data and workshops: the scale and timing of the incident; the size of the victim organisation; the level of preparation undertaken by the victim organisation prior to the ransomware event; the nature of the existing workplace culture; the experience dealing with third parties; the role of communications; and the role of transparency and information sharing. Figure 1 illustrates how the various elements interact.

The Scale, Timing and Context of the Incident

The victim experience naturally depends on the scale and technical impact of the incident: the percentage and type of data encrypted, locked or exfiltrated might vary. A victim in the education sector, for example, found that all email servers and backups were encrypted but their database was not affected.[23] Other interviewees experienced breaches that resulted in the encryption of core company systems, creating significant business interruption and organisation-wide disruption.[24] The nature of the exfiltrated data may have a significant influence on the victim experience, especially where it involves the compromise of sensitive data.[25] In other instances, the threat actors either did not exfiltrate data or siphoned

23. Author interview with Education 1, 8 December 2022.
24. Including but not limited to: author interview with Manufacturing 1, 27 January 2023; author interview with Technology 3, 24 March 2023; author interview with Government Agency 1, 3 March 2023; author interview with Local Government 1, 15 December 2022; author interview with Local Government 2, 1 March 2023; author interview with Education 2, 16 December 2022.
25. Author interview with Local Government 1, 15 December 2022; author interview with Outsourcing 1, 15 December 2022.

Figure 1: Factors Shaping the Ransomware Victim Experience



Source: The authors.

data that was of little material concern to the victim organisation. An interviewee from the education sector recalled their relief when the threat actors only threatened to release generic invoices rather than sensitive student data.[26]

The timing of an incident further influences the damage to victims and their ability to successfully respond to the attack. Many cybercriminals are known to time their attacks to inflict the maximum harm on victims. This increases the pressure to pay ransoms. For example, an attacker may launch attacks against the education sector at the beginning of a term or during exam periods.[27] Additionally, prominent ransomware criminals are typically located in different time zones from their victims,[28] naturally facilitating 'out-of-office attacks'. Several interviewees reported that they were made aware of a successful breach during

26. Author interview with Education 2, 16 December 2022.
27. Nicole Sganga, 'Ransomware Group Vice Society Targeted Dozens of Schools in 2022, New Report Finds', *CBS News*, 6 December 2022.
28. Renee Dudley, 'Who are the Ransomware Gangs Wreaking Havoc on the World's Biggest Companies?', *The Guardian*, 17 July 2023; NCC Group, 'Threat Intelligence Report', January 2024, <https://www.nccgroup.com/media/xmonzne2/jan-24-threat-report-digital.pdf>, accessed 10 June 2024; Check Point, 'March 2024's Most Wanted Malware: Hackers Discover New Infection Chain Method to Deliver Remcos', 9 April 2024, <https://blog.checkpoint.com/security/march-2024s-most-wanted-malware-hackers-discover-new-infection-chain-method-to-deliver-remcos/>, accessed 10 June 2024.

the night or while on annual leave.[29] A common, although not universal, perspective was that the first tangible signs of a spreading encryption payload were the takedown of monitored on-site health and safety systems, including fire alarms and CCTV.[30]

The Covid-19 pandemic substantially shaped the external context for many victims. Some interviewees found that pandemic-related IT and work-from-home practices had made them more resilient, as much data had been moved to the cloud and people were accustomed to remote working or learning.[31] For an interviewee in local government, the pandemic tested skills that were similarly required in responding to the attack – it was therefore a useful point of reference.[32] Others found that the pandemic and their ransomware incident had a cumulative negative impact on themselves or their colleagues. For example, for one victim, pandemic-related practices had already cost staff much energy and resources and the incident thus came at a time when 'people were already [at] rock bottom in terms of morale and resilience'.[33] New working patterns established during the pandemic also made one victim's IT estate more vulnerable as many devices were no longer switched off regularly due to remote working and did not therefore automatically update.[34]

However, the timing of an incident may, or may not, also coincide with internal procedures – this has an impact on how harmful the experience is for victims. While it might seem odd to speak of an 'ideally timed' ransomware incident, timing can reduce possible negative experiences. For example, several victims reported that their incidents hit just after they had made payroll.[35] Had they been unable to pay their employees, the harm for those individuals as well as the victim organisation would have been greater. Another victim experienced fortunate timing as the attack hit them several months after the organisation had run cyber exercises that resulted in hiring experts trained in responding to cyber incidents.[36] As noted above, others had recently moved their systems to the cloud, ensuring access after the ransomware breach, thus alleviating some of the harm.[37] In other cases, victims felt that the timing of the ransomware

29. Author interview with Education 1, 8 December 2022; author interview with Education 3, 10 January 2023; author interview with Government Agency 2, 3 March 2023.
30. Author interview with Education 2, 16 December 2022; author interview with Education 3, 10 January 2023.
31. As was the case described in author interview with Education 4, 10 March 2023.
32. Author interview with Local Government 1, 15 December 2022.
33. Author interview with Education 4, 10 March 2023.
34. Author interview with Charity 1, 12 January 2023.
35. Author interview with Education 3, 10 January 2023; author interview with Technology 3, 24 March 2023.
36. Author interview with Engineering 1, 10 March 2023.
37. Author interview with Outsourcing 1, 15 December 2022.

incident was particularly bad, with their breach occurring at a time of low budgets[38] or acutely low staff morale.[39]

How much an organisation depends on its IT infrastructure or how time-sensitive its business is may also influence the degree of harm and disruption that the organisation and/or its staff experience. Victims operating in acutely time-sensitive client-facing contexts may lose contracts if they are unable to resume operations within a matter of days.[40] In such contexts, the high stakes of an acutely time-sensitive incident response elevate pressure on colleagues handling the response effort. On the other hand, other interviewees reported that they had the (relative) luxury of time in their recovery effort.[41]

The timing, scale and context of the ransomware attack are therefore significant factors influencing the harm caused to and the fallout experienced by an organisation and its staff. Policymakers, business leaders and practitioners thus need to consider that while victims share similar experiences, individual circumstances and the extent of the attack heavily influence how much a victim is affected. These factors also contribute to how personally a ransomware incident is felt by its victims, a sentiment that was repeated throughout this research.

Size of Organisation

The size of a company can also influence the extent of the impact in a ransomware attack. This has also been confirmed in other reports.[42] While larger companies typically operate a more expansive IT estate – which may include layers of end-of-life software – such organisations are likely to offset associated risks through their access to greater cash reserves either to pay a ransom and/or afford third-party help. They might also have a designated IT team, incident responders or lawyers on retainer and generally have greater experience in crisis management. This makes larger companies more resilient and less dependent on publicly available resources and expertise. Smaller companies or sole traders, however, may lack designated IT staff, the resources or the experience to successfully manage a ransomware attack. As a result, a ransomware attack can be significant, if not existential to small and medium-sized enterprises (SMEs), which are often

38. Author interview with Local Government 2, 1 March 2023.
39. Author interview with Professional Services 1, 17 March 2023.
40. Author interview with Insurance Claims 3, 3 February 2023.
41. Author interview with Charity 1, 12 January 2023.
42. Quinn Cleary, 'The Devastating Impact of Ransomware Attacks on Small Businesses', University of Maryland Francis King Carey School of Law, 4 April 2023, <https://www.law.umaryland.edu/content/articles/name-659577-en.html>, accessed 10 June 2024; Jen Matteis, 'How Ransomware is a Big Problem for Small Business – And What to Do About It', Insureon, 10 July 2023, <https://www.insureon.com/blog/how-ransomware-is-a-big-problem-for-small-business>, accessed 10 June 2024.

more dependent on public resources and expertise.[43] One interviewee who provides third-party services said that the impact on lives is particularly prevalent for very small business, for example where a couple are in business together and all their assets and income depend on that business.[44] The interviewee found that 'the existential threat for a business that's much smaller is significant'.[45] An interview with a micro-SME victim suggested that without the financial support and access to expertise provided through a cyber insurance policy, the firm would have ceased to trade and the business owner would have needed to sell their home.[46] Additional pressure may arise for small business owners for whom their livelihoods and those of their employees are at stake.[47]

While limited in its insights on small business owners, the interview data raises questions about the impact of a company's size on the harm experienced by ransomware victims. This has also been addressed in public reports, such as the news reports on the ransomware attack against hospitality and casino giant MGM Resorts. Such reports have questioned whether the company was 'too rich to ransomware', arguing that the impact was lower because of its large size.[48] In contrast, other studies underline the disproportionate effect that is felt by small business owners or sole traders who become ransomware victims.[49] While individuals working in large or small organisations may experience similar harm, such as psychological, on an individual level organisational size matters in terms of the financial harm and potential existential risk an organisation faces. Policymakers must consider that, to limit the harm felt by ransomware victims, organisations of different sizes might require different types and levels of government support in responding to ransomware attacks.

Level of Preparation

An organisation's level of preparation prior to the incident is a significant factor determining the harm that a victim experiences.[50]

43. Christine Ro, 'Why Some Cyber-Attacks Hit Harder than Others', *BBC News*, 23 February 2024.
44. Author interview with Digital Forensics and Incident Response (DFIR) 2, 6 December 2022.
45. *Ibid*.
46. Author interview with Consultancy 2, 17 March 2023.
47. Author interview with Insurance Claims 2, 19 January 2023.
48. Becky Bracken, 'Too Rich to Ransomware? MGM Brushes off $100M in Losses', *Dark Reading*, 6 October 2023, <https://www.darkreading.com/attacks-breaches/too-rich-to-ransomware-mgm-brushes-off-100m-in-losses->, accessed 10 June 2024.
49. Swiss Re, 'SMEs are Particularly Vulnerable to Cyber Attacks', 9 November 2022, <https://www.swissre.com/risk-knowledge/advancing-societal-benefits-digitalisation/SMEs-are-particularly-vulnerable-to-cyber-attacks.html>, accessed 10 June 2024; John Griffin Jr, 'Be Ransom Wary: How Small Businesses are Vulnerable to Cybercrime', *Forbes*, 14 January 2022.
50. Author interview with Insurance Claims 2, 19 January 2022.

The existence and suitability of business continuity plans, for example, was repeatedly cited throughout the research project.[51] The general assumption is that when an organisation has a 'good resilience strategy, they can put in place a recovery process that would take days as opposed to weeks' and that such measures would allow them to resume services and thereby 'minimise impact to the individual consumers'.[52] While many interviewees stressed the importance of preparation to limit the harm ransomware attacks cause, this research project also found that many doubted the suitability of existing business continuity plans to respond to a ransomware attack. Business continuity plans for flooding or fire emergencies have little in common with those setting up response mechanisms to a ransomware or other cyber incident. As a victim in the education sector described: 'people always have … business continuity plans … but actually they tend to go out of the window'.[53]

Business continuity plans for incidents other than ransomware or IT outages often presume that IT systems, such as email, continue to function and can be used to facilitate the crisis response. In practice, however, it is often the case that 'There is no email. There is no Excel. Think pencil. Think paper'.[54] Another interviewee noted that for 'traditional', more routine crises, they would typically bring in contractors to resolve the issue and pay them through the invoicing system, which was no longer possible during the incident.[55]

Specific preparation for a cyber incident, by pre-emptively increasing 'resilience', can help alleviate the harm victims experience. Business continuity plans need to be tailored, while retaining sufficient flexibility to adapt to variables such as the threat actor, attack modality, severity and scale of encryption or exfiltration.

One way to prepare is by identifying essential systems for core organisational functionality. This guides the victim to set priorities for their incident response.[56] A victim in the education sector, for example, stressed the importance of the student portals to enable students to study for exams.[57] An incident responder recalled their experience of supporting a manufacturer, who insisted that their canteen facility must be restored as an urgent priority in the interests of maintaining staff morale.[58]

Another way to prepare is by running scenario tests, as undertaken by a victim in the engineering sector, who subsequently hired additional staff as a result of the exercise, whom they described as 'absolutely critical' in the response to the

51. *Ibid.*
52. Author interview with DFIR 3, 12 December 2022.
53. Author interview with Education 3, 10 January 2023.
54. *Ibid.*
55. Author interview with Manufacturing 1, 27 January 2023.
56. Author interview with Ransomware Specialist 3, 7 March 2023.
57. Author interview with Education 1, 8 December 2022.
58. Author interview with DFIR 2, 6 December 2022.

ransomware incident the company experienced a few months later.[59] A ransomware specialist mentioned pre-drafted communications and legal statements as a proactive way to successfully prepare for a ransomware attack.[60] Several interviewees stressed that the ransomware business continuity documents themselves should be stored offline in analogue format to ensure access is possible following an encryption event.[61] Policymakers and those trying to raise awareness and preparation levels among potential victims must thus continue to stress the importance of cyber-specific preparation that takes into account the unique features of a cyber incident instead of relying on generic contingency plans that are unsuitable in a digitalised context.

Specific preparation for a cyber incident is tightly linked to the overall level of cyber hygiene and cyber awareness a victim organisation may have prior to the incident. As one interviewee from the technology sector pointed out, preparatory measures are 'far more effective than just leaning in after the incident'.[62] Particularly in the public sector, however, digitalisation has been a lengthy process. One victim described how in their institution they had to recover server-by-server as the integration between devices and data flows were 'a nightmare'.[63] Similarly, another victim from the education sector described how, at an earlier point, they used technology, but that they had 'not paid enough attention to the kind of infrastructure and the security' that was needed.[64] In hindsight, they said that they should not have been running old systems and ought to have allocated the budget 'to do it properly'.[65] However, this has financial implications. In the private sector, there are also examples of missing cyber security measures. An interviewee from the technology sector, for example, admitted that 'probably there were things that we knew we should improve but because we were so busy we didn't do them'.[66]

This may include the availability and quality of backups,[67] particularly ones that are offline. An external counsel described a situation where there are no viable backups as the 'worst case'. They stressed that such a difficult situation may be business critical and lead victims to consider paying the ransom where attempts to recover the data from other sources are unsuccessful.[68] Furthermore, good

59. Author interview with Engineering 1, 10 March 2023.
60. Author interview with Ransomware Specialist 3, 7 March 2023.
61. Author interview with Charity 1, 12 January 2023; author interview with Manufacturing 1, 27 January 2023.
62. Author interview with Technology 1, 20 March 2023.
63. Author interview with Education 3, 10 January 2023.
64. Author interview with Education 4, 10 March 2023.
65. *Ibid.*
66. Author interview with Technology 3, 24 March 2023.
67. Author interview with DFIR 6, 1 February 2023.
68. Author interview with External Counsel 2, 14 December 2022. In the interview with DFIR 5, 23 January 2023, the interviewee confirmed that the worst incident they encountered was one where the backups were also wiped out.

detection capabilities may enable a victim to identify the attack early and take measures to mitigate further harm or even disrupt the attacker. Such damage limitation can significantly reduce the severity of the overall incident.[69]

Finally, a good awareness of the amount and kind of data an organisation stores helps it to react to the incident. One interviewee from law enforcement pointed out that many organisations do not 'really realise how sensitive some of the data is that they hold'.[70] They added that smaller organisations, as well as those from the public sector, are particularly impacted by ransomware attacks due to the type of data they hold. The interviewee gave an example of a law firm holding data on victims of sexual offences and people being accused of being sex offenders. As a consequence, 'each individual person within that dataset became quite vulnerable quite quickly … because their names should never be released'.[71] Similarly, an interviewee with third-party experience from the insurance sector found that unnecessarily holding a lot of personal data would be a factor that aggravates the victim experience, while good data management practices such as deleting data they no longer need or should not have can reduce that risk.[72]

General cyber security hygiene, good data privacy practice and specific cyber incident preparation can alleviate the harm experienced. Policymakers and public institutions must continue to raise awareness of such measures, particularly for small and micro-enterprises. When determining budgets for often tightly resourced public service providers, policymakers must allocate a budget for digitalisation and modernisation that goes beyond purchasing new technological equipment and considers the implementation and continued evaluation and adaption of cyber security standards. This also means that it is necessary to invest in adequate training or hiring dedicated IT staff.

Pre-Existing Workplace Culture

The interview data highlights the importance of the pre-existing workplace culture in aggravating or limiting ransomware harm. A ransomware attack is likely to intensify existing sentiment within and between teams. As one interviewee stated:

> the stronger [the] 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 for

69. Author interview with Engineering 1, 10 March 2022.
70. Author interview with Law Enforcement 1, 9 December 2022.
71. *Ibid.*
72. Author interview with Insurance Claims 1, 14 December 2022.

> whatever those reasons might be, you're particularly vulnerable to this having a disproportionate effect on morale.[73]

Another interviewee, from a local government organisation, confirmed that the attack 'definitely exacerbated areas where there were tensions anyway'.[74]

One interviewee went as far as stating that a good workplace culture has a greater impact on the ransomware victim experience than 'a really well-prepared tech system', as morale and culture cannot be replaced but may have a disproportionate impact on people's resilience.

A decisive factor is the overall atmosphere and level of cooperation among co-workers. A victim in the education sector spoke of a 'real good spirit' among the team in response to the attack: people even wanted to help and unexpectedly came into the office, bringing cookies and cake.[75] In this example, the interviewee stated that the ransomware attack brought the team really 'close to each other in the end' and such bonds have continued to benefit the team spirit.[76] Similarly, another interviewee in the education sector referred to an experience that strengthened the ethos at work like a 'wartime spirit. Everybody pulled together'.[77] A similar observation was made by participants from the local government sector.[78]

Interviewees linked the two themes of organisational preparation and pre-existing workplace culture. This identified the need for a clear allocation of jobs and responsibilities.[79] Where tasks were clearly attributed, victims experienced less chaos and seemed to better stay on top of the incident, an important factor contributing to the maintenance of morale and the reduction of harm. It also helps to avoid duplication of efforts, which can be especially costly when hired third parties are involved.[80] Additionally, the allocation of tasks should be accompanied by situational awareness; this reinforces the utility of pre-incident wargaming. An incident responder highlighted that chief information security officers (CISOs) and data protection officers were acutely at risk of being overwhelmed. They recalled a typical case where the CISO was 'this one guy in the middle, who was the fundamental access point for all of the activity'.[81]

The allocation of jobs is closely linked to the reaction of, and leadership from, senior management and the board. Their role can help to alleviate harm or add additional burden. A victim in the technology sector felt that 'we were ill equipped

73. Author interview with Professional Services 1, 17 March 2023.
74. Author interview with Local Government 1, 15 December 2022.
75. Author interview with Education 1, 8 December 2022.
76. *Ibid.*
77. Author interview with Education 2, 16 December 2022.
78. Author interview with Local Government 2, 1 March 2023.
79. Author interview with Insurance Claims 2, 19 January 2023.
80. Author interview with Technology 2, 21 March 2023.
81. Author interview with DFIR 4, 14 December 2022.

at senior leadership level to deal with this', particularly regarding job allocation.[82] An incident responder went as far as to say that the technical response to an incident is the easy part and that, instead, leadership rather than technical expertise is the overriding factor.[83] A ransomware specialist explained that 'one thing that makes [the experience] better is a strong CEO leadership or a strong senior board leadership, making a decision right at the beginning how they're gonna deal with this and taking responsibility'.[84] For example, the board may take additional action to support the incident response team. One interviewee explained how the chairman provided an additional office freezer for ice-cream, which was intended to be gentle on the stomach during late-night working.[85] Conversely, the coordinator of a ransomware response at a charity organisation resented that senior management did not offer use of an existing apartment in the office building for rest and food consumption.[86] In their case, the combination of lack of sleep, poor nutrition and excessive consumption of caffeine necessitated a visit to A&E.[87]

The extreme exertion that may be required to recover from ransomware[88] – especially for IT staff[89] – supports the organisation but may degrade the wellbeing of staff through sleep deprivation, physical inactivity, poor nutrition and strained relationships.[90] As the primary interest of the board or trustees often remains the financial impact on an organisation, there is a risk of overlooking the physiological and psychological impact the ransomware attack might have on individuals.[91] As an indication of a common trend, one IT expert in the charity sector stressed that they would have liked to see more support from senior management, for example with respect to looking after the health of the core team responding to the incident.[92]

This is not isolated to the ransomware crisis itself and can include a post-ransomware workplace legacy. One victim described how, after the incident had been resolved, they had to work harder and took longer to do tasks due to additional fail-safes, for example when manually creating reports that were

82. Author interview with Technology 2, 21 March 2023.
83. Author interview with DFIR 1, 5 December 2022.
84. Author interview with Ransomware Specialist 1, 12 December 2022.
85. Author interview with Engineering 1, 10 March 2023.
86. Author interview with Charity 1, 12 January 2023.
87. *Ibid.*
88. Author interview with Engineering 1, 10 March 2023; author interview with Charity 1, 12 January 2023.
89. Pia Hüsch, Jamie MacColl and Gareth Mott, 'The Human Toll of Ransomware: How IT Pros Suffer During Incidents', *Computer Weekly*, 16 January 2024.
90. Author interview with Engineering 1, 10 March 2023; author interview with Charity 1, 12 January 2023; author interview with Financial Services 1, 9 December 2022.
91. MacColl et al., 'The Scourge of Ransomware'.
92. Author interview with Charity 1, 12 January 2023.

normally done automatically.[93] They added that they felt that 'nobody cared that we were working harder' as the bottom line was the core concern.[94] Messaging from senior leadership can also influence staff morale and the working environment during and after a ransomware event. Particularly where cyber awareness is low, board members or trustees might engage in a culture of blame,[95] for example by accusing the IT team of failing to do its job. One victim described how there was no clear messaging from leadership, for example on communication about the incident.[96] Given the lack of cyber awareness among senior staff members, IT staff also, at times, find themselves 'leading the charge', as a victim in the charity sector explained.[97]

Conversely, the role of senior management might be proactive and supportive, realising that a ransomware attack is not just an IT problem.[98] In these cases, senior management can prevent burnout of team members, making sure to rotate staff and providing them with time off. In local government, for example, staff of a victim organisation were given extra holidays and paid time off once the immediate response was over.[99]

This highlights that responding to a ransomware attack must be thought of as a marathon, not a sprint. Many interviewees and, particularly, incident responders and external counsels stressed this point. Some of them highlighted that one of the first things they do is advise on the need to rotate staff and prevent burnout.[100] This is true for staff at the victim organisation, but equally applies to third parties, such as incident responders. Such responders run a high risk of burnout and therefore need to rotate between incidents or have leave provided to limit the stress they experience.

The general workplace culture is therefore a critical factor that determines how victims perceive a ransomware incident. While policymakers and cyber security professionals cannot have an impact on workplace culture, they can stress the important role that it plays in preparing for, and responding to, incidents. This includes drawing attention to the critical role of senior management and board members in managing the ransomware incident. Awareness and educational training must highlight the positive effects that stem from a clear division of tasks and vision for the response. Furthermore, awareness campaigns and best-practice guidance can outline practical examples of how to provide support for

93. Author interview with Manufacturing 1, 27 January 2023.
94. *Ibid.*
95. Author interview with Ransomware Specialist 3, 7 March 2023.
96. Author interview with Charity 1, 12 January 2023.
97. *Ibid.*
98. Author interview with Insurance Claims 3, 3 February 2023.
99. Author interview with Local Government 2, 1 March 2023.
100. Author interview with DFIR 2, 6 December 2022.

the core response team and avoid a culture of blame. Boards and senior management must also be cyber aware – this is a key aspect of an existing work culture that can contribute to alleviating the ransomware harm. New legal obligations and/or training of boards and senior management can achieve this.

Paying (or Not Paying) a Ransom Demand

Interviewees frequently spoke of the influence of ransom payments on the victim experience. The project team interviewed individuals from both ransom-paying and non-paying victim organisations. Only a minority of victim organisations who took part in the interviews paid ransoms.[101] Two interviewees noted that their organisation made a ransom payment because it was the most efficient solution to decrypt affected systems in an acutely time-sensitive context. Another interviewee noted that their organisation had paid a ransom because they were very keen to dissuade the threat actors from releasing sensitive exfiltrated data.[102] While the overall number of ransom-payers is limited relative to the number of interviewees, there are nonetheless significant insights that can be gleaned from the role that ransom payment (or non-payment) has in influencing the ransomware victim experience. Importantly, apart from select government or law enforcement interviews, interviewees were typically not directly asked about the morality of ransom payments or whether ransom payments should be permitted or prohibited. Rather, the focus was on the experience of paying (or not paying) a ransom and how this positively or negatively impacted the victim's journey through a ransomware incident.

In the cases above, the payment of the ransom significantly alleviated the harms experienced. Payment of the ransom meant, for example, that students were able to complete their exams in the usual way. This would not have been possible if the victim, who came from the European education sector, had sought to restore systems without a decryption key.[103] For a victim working in the technology sector, the ransom payment was the only viable option to keep the company afloat.[104] For the outsourcing firm, the payment of the ransom meant that, at least at the time of writing, the threat actors had not released exfiltrated data.[105]

101. This is likely due to bias in the project's interview data. The data comprises few private sector victims, especially small businesses, and more public sector victims. This is more likely due to their policies rather than any ability to pay. Other studies have found that the percentage of victim organisations paying ransom is much higher. One study points to 82% of UK ransomware victim organisations paying ransom. See *BBC News*, 'Study: UK Firms Most Likely to Pay Ransomware Hackers', 23 February 2022.
102. Author interview with Outsourcing 1, 15 December 2022.
103. Author interview with Education 1, 8 December 2022.
104. Author interview with Technology 3, 24 March 2023.
105. Author interview with Outsourcing 1, 15 December 2022.

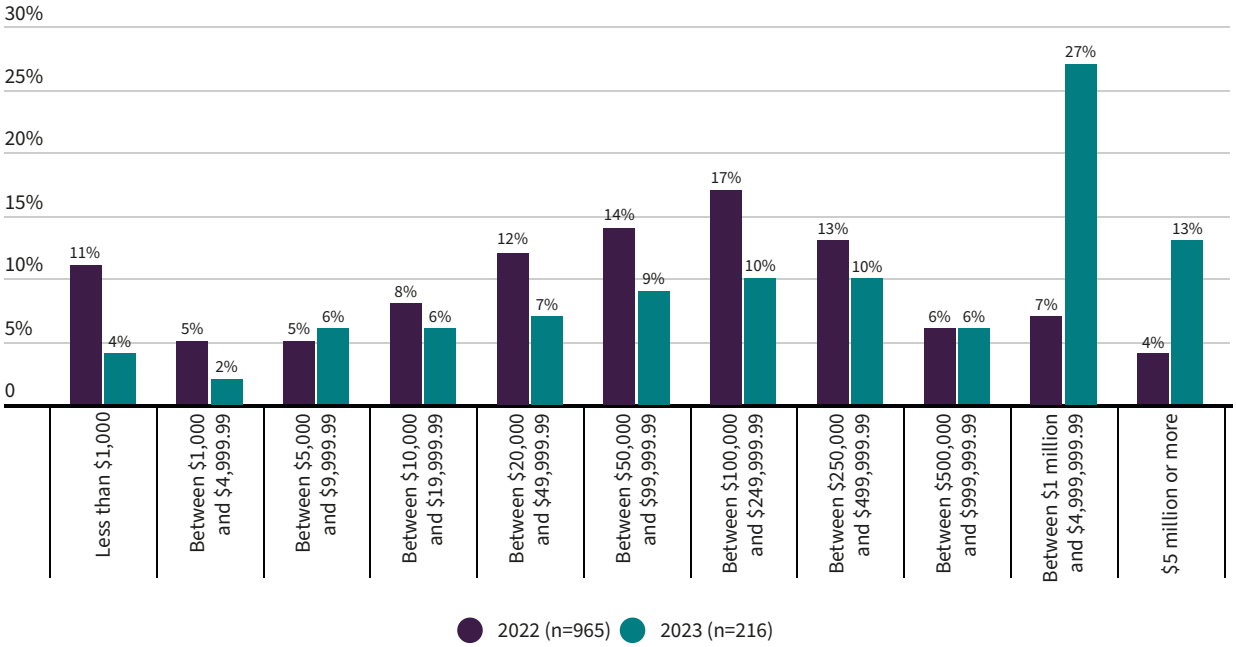
While anecdotal, these case studies highlight that, in some situations, the payment of a demanded or negotiated ransom can significantly alleviate harms.

It is, however, important to note that interview data also highlighted that a ransom payment is not a silver bullet. A ransomware negotiator noted that in their experience, all ransomware operators will eventually 'go rogue'.[106] For example, they may re-extort from the same victim after a ransom payment has been made, they may not deliver operable decryption keys, or they may renege on promises and release or sell exfiltrated data.[107] Other studies have confirmed such outcomes, finding that a high percentage of victims who pay are victimised again.[108] Similarly, studies report that not everyone paying a ransom actually recovers their data.[109] In this light, whether a ransom payment successfully alleviates the harm that is experienced depends on the good faith of the ransomware operators and the technical efficacy of their malware (and decryption keys).

Additionally, it is important to note that the payment of a ransom does not absolve a victim organisation of its obligations to report the incident to the ICO; the breach has still occurred.[110] The compounding of reputational risk was cited as a concern. Non-paying victims noted that there was a stigma attached to paying organised criminals a ransom and noted that had they made a payment, it would have adversely affected their relationship with clients or other stakeholders.[111] The logistics of making the ransom payment, including accessing large quantities of Bitcoin, can also be challenging. One ransom payer recalled that the process of multiple bank authorisation checks to purchase increments of Bitcoin was arduous and compounded their stress.[112] It is worth noting that UK banks have increasingly prohibited customer access to cryptocurrency exchanges.[113]

106. Author interview with Ransomware Specialist 3, 7 March 2023.
107. *Ibid*.
108. For further information on second ransomware attacks after first ransom payment see, for example, Eileen Yu, 'Most Firms Face Second Ransomware Attack After Paying off First', *ZDNet*, 16 June 2021.
109. Nolen Scaife, Patrick Traynor and Kevin Butler, 'Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)', *IEEE Potentials* (Vol. 36, No. 6, 2017), pp. 28–31; Davey Winder, 'Ransomware Reality Shock: 92% Who Pay Don't Get Their Data Back', *Forbes*, 2 May 2021.
110. Author interview with Insurance Claims 1, 14 December 2022; author interview with External Counsel 4, 2 March 2023. See also Information Commissioner's Office (ICO) and NCSC, 'Re: The Legal Profession and its Role in Supporting a Safer UK Online', letter addressed to Stephanie Boyce, Mark Fenhalls and colleagues, 7 July 2022, <https://www.ncsc.gov.uk/files/Joint-ICO-and-NCSC-letter-to-The-Law-Society-and-The-Bar-Council.pdf>, accessed 21 May 2024.
111. Author interview with Local Government 1, 15 December 2022; author interview with Education 3, 10 January 2023; author interview with Government Agency 2, 3 March 2023.
112. Author interview with Technology 3, 24 March 2023.
113. Jack Schickler, 'UK Banks Blocking Crypto Access Given Fraud, Volatility, Lawmakers Told', *CoinDesk*, 7 February 2023, <https://www.coindesk.com/policy/2023/02/07/uk-banks-blocking-crypto-access-given-fraud-volatility-lawmakers-told/>, accessed 23 February 2024.

Figure 2: Ransomware Payments in 14 Select Countries in 2022 and 2023 ($)



Source: Sophos, 'The State of Ransomware 2023', Sophos Whitepaper, May 2023, <https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf>, accessed 10 June 2024.

The decision on whether to pay a ransom weighed heavily on victims. Of course, paying a ransom is also a financial decision (see Figure 2), but whether to pay a ransom also raises other considerations for victims. An interviewee from a victim organisation that elected to pay a ransom noted that the decision-making was difficult and stressful for the executive board.[114] A ransomware specialist noted that victim organisations that agonise over whether to pay a ransom prolong the initial (and most stressful) crisis phase of the ransomware event.[115] Conversely, those that quickly ruled out a ransom payment were able to focus their energy on the rebuild.[116]

The payment of a demanded or negotiated ransom can thus both positively and negatively influence the ransomware victim experience. Preparedness is important.[117] This should include delegating decisions to individuals to make payment decisions. Organisational leadership must also bear in mind that the payment of a ransom does not guarantee restoration of access to encrypted files or systems, nor the deletion of exfiltrated data. It is also important that organisations adhere to local regulations on reporting and sanctions compliance.

114. Author interview with Education 1, 8 December 2022.
115. Author interview with Ransomware Specialist 1, 12 December 2022.
116. *Ibid.*
117. Views expressed by Government 1, November 2022 workshop.

Experience of Dealing with Third Parties in the Ransomware Response Ecosystem

This section looks at some of the third parties a ransomware victim might typically be in contact with when reacting to a ransomware attack and further explores the degree to which these interactions influence the victim experience. Given the key role of law enforcement and other public sector service providers, Chapter III is dedicated to their impact on the victim experience.

How organisations interact with third parties in the ransomware ecosystem is an essential component of the victim experience. Some victims have a very positive experience in their engagement with external parties. One victim in the private sector stressed that 'we were really looked after'.[118] Others gave less credit to external parties and stressed that, ultimately, they were alone in the experience.[119] The interview data confirms that the interaction with third parties is an important factor for the victim experience.[120] As a ransomware specialist phrased it: 'harm does get amplified if [victims] don't have good advice'.[121]

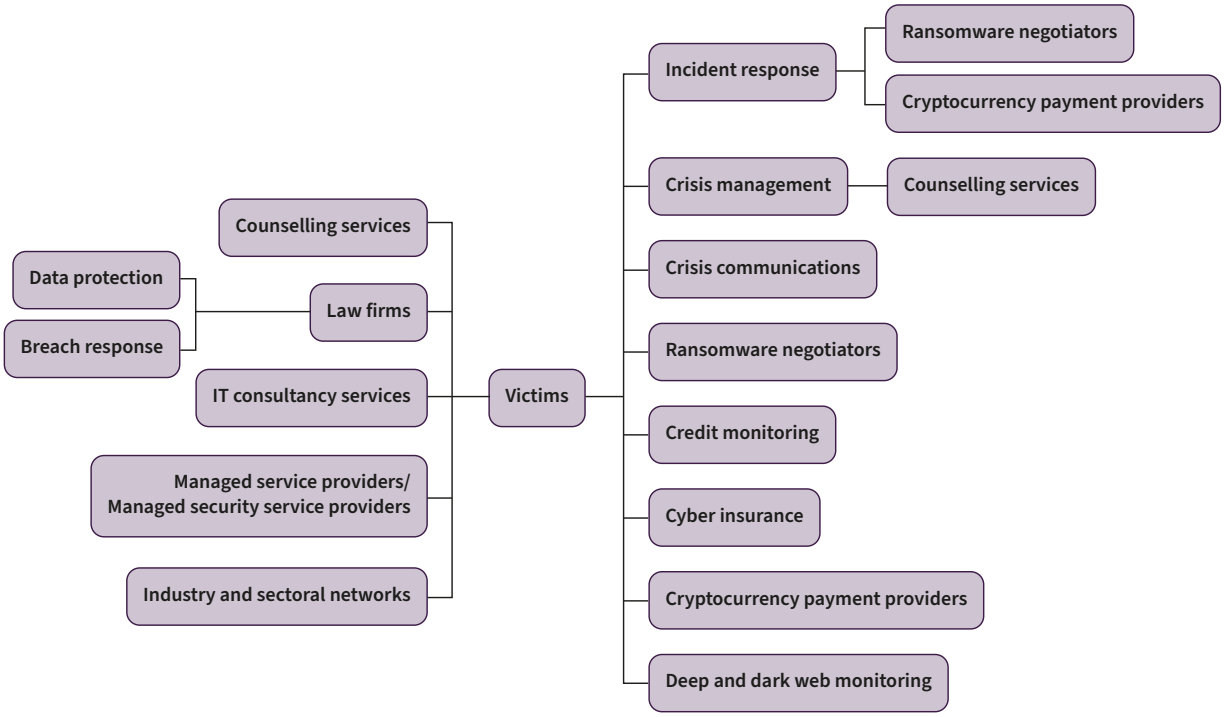
Some of the key third parties and their services are highlighted in Figure 3 and explored in the following sections.

Lawyers

Many victims acknowledged that legal advice on the repercussions of a ransomware attack is necessary, particularly on the implications of the data breach and potential lawsuits that might cause further harm. Increasingly, however, lawyers are consulted at the very beginning of an incident and subsequently manage relationships with all parties involved.[122] One victim said lawyers helped with the risk assessment for exfiltrated data, particularly to assess the scope of potential lawsuits coming from those whose data has been exfiltrated.[123] However, as lawyers are often tasked with avoiding potential further harms, their positive impact may be less tangible for victims. Additionally, lawyers typically work to protect the organisation as a single entity, rather than the individuals connected to it. Here, again, the interview data may speak to a dichotomy between the

118. Author interview with Consultancy 2, 17 March 2023.
119. Author interview with Professional Services 1, 17 March 2023.
120. Author interview with Insurance Claims 2, 19 January 2023; author interview with Ransomware Specialist 1, 12 December 2022.
121. Author interview with Ransomware Specialist 1, 12 December 2022.
122. Daniel Schwarcz, Josephine Wolff and Daniel W Woods, 'How Privilege Undermines Cybersecurity', *Harvard Journal of Law & Technology* (Vol. 36, No. 2, Spring 2023), pp. 421–86.
123. Author interview with Outsourcing 1, 15 December 2022.

Figure 3: Examples of Private Sector Third Parties Offering Victims Services and Support



Source: The authors.

success and failure of the organisation and the real-time experiences of staff at the organisation. Some victims conveyed a negative experience dealing with lawyers, primarily stressing that the involvement of a legal team often meant that lawyers limited communications and information sharing about the incident – including as a precaution due to perceived legal risks.[124] A victim in the education sector confirmed that the legal team was 'really tight on what we could and couldn't say'.[125] This meant that they could only communicate that there was a cyber attack, but not a ransomware attack, which 'made things hard at times'.[126] One victim also felt that restrictions imposed by the legal team prevented them from sharing information, for example sharing technical indicators with the NCSC.[127] Others also reported that they were unable to share information, and therefore were unable to warn colleagues in other institutions. This led to feelings of guilt when a later attack against an acquaintance might have been prevented had a warning been shared.[128]

The impact of legal wraparound on the ability of victims to share their experiences was also noticed by an interviewee from law enforcement. They stated that they 'definitely found it hard to engage with organisations freely once a law firm

124. Author interview with Education 3, 10 January 2023.
125. *Ibid.*
126. *Ibid.*
127. Author interview with Technology 2, 21 March 2023.
128. See Internal and External Communications section; author interview with Education 3, 10 January 2023.

becomes involved'.[129] While they respected the lawyer's prerogative to act in the best interest of their clients, the law enforcement interviewee nevertheless felt that it impacted their ability to 'respond effectively', for example, because they cannot take down an exfiltrated dataset if they do not know about it.[130]

Lawyers therefore reduce the harm to individuals and organisations in less tangible ways, for example by preventing future lawsuits. However, their concern over the legal implications stemming from oversharing information limits information and knowledge exchange. Their requirements to tightly control information are therefore perceived to potentially contribute to strained experiences.

Insurance Providers

Although most organisations do not have cyber insurance,[131] interviewees from organisations that did were overwhelmingly positive about their interactions with cyber insurance providers. Interviewees credited their coordinating function and their ability to convene appropriate external service providers at speed. For example, one victim was 'amazed at the scale and quality of support that was very quickly in place'.[132] Another victim confirmed the central role of their insurance provider in the steering process, stating that without that service the start of recovery would have been delayed and taken a lot longer.[133] Similarly, another victim confirmed that without insurance they would not have known how to find the right experts and would have taken much more valuable time to do so, describing having cyber insurance as 'absolutely pivotal'.[134]

This data confirms the central role of insurance providers in coordinating the ransomware response and correlates with similar findings from prior research.[135] There were two core benefits. First, access to a support network: 'it's the expertise and the people and how quickly you can assemble the team'.[136] The value of cyber insurance in helping to manage the response is particularly important for smaller organisations given they are much less likely to have incident response or legal

129. Author interview with Law Enforcement 1, 9 December 2022.
130. *Ibid.*
131. Department for Science, Innovation & Technology, 'Cyber Security Breaches Survey 2023', 19 April 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023#summary>, accessed 10 June 2024.
132. Author interview with Outsourcing 1, 15 December 2022.
133. Author interview with Charity 1, 12 January 2023.
134. Author interview with Professional Services 1, 17 March 2023.
135. Gareth Mott et al., 'Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era', *Computers & Security* (Vol. 128, May 2023), pp. 1–21; Daniel W Woods and Rainer Böhme, 'How Cyber Insurance Shapes Incident Response: A Mixed Methods Study', paper presented at the 20th Annual Workshop on the Economics of Information Security, online, 28–29 June 2021.
136. Author interview with Technology 3, 24 March 2023.

services on a retainer. Second, insurance provides access to a financial cushion: for example, one interviewee described the benefit of cyber insurance as allowing the company to respond to the attack without concerns over cost.[137] Another victim, the director of a micro-SME, found that having insurance 'saved everything', and that without it 'it would have been totals', including the need to sell their home.[138]

The support and experience of insurance providers might also alleviate some of the stress and mental harm experienced by victims. One victim added that they were impressed that the insurers 'were completely unflappable. They stood behind us straight away'.[139]

Incident Responders

Interviewees painted a mixed picture with respect to the impact of incident responders. They were generally perceived as providing critical work limiting the – often technical – harm that victims experienced. This is especially true for organisations that do not have in-house IT teams with experience of handling ransomware incidents. Such organisations may feel that they are out of their depth in dealing with a ransomware incident.

However, the context of external incident response support matters. One incident responder confirmed that in the past six months they were the second firm to be called to a case for roughly 50% of their ransomware cases.[140] Some incident responders may not be well-aligned with the IT infrastructure of the victim organisation; in one cited example, an incident responder required several days to patch the client's IT systems so that it could connect to the response firm's forensic software.[141] Other incident responders might lack the experience that can be acquired from handling high caseloads to result in the most efficient and effective path. An incident responder concluded that they had 'seen some awful, awful aftermaths of either bad breach counsel, bad PR [and] even bad recovery'.[142] Comments such as these stressed that third parties, including incident responders, can aggravate the harm victims experience when they provide a poor service, increasing the victim's operational downtime and potentially forcing victims to reach out to a second incident responder for an expedited resolution.

137. Author interview with Professional Services 1, 17 March 2023.
138. Author interview with Consultancy 2, 17 March 2023.
139. Author interview with Professional Services 1, 17 March 2023.
140. Author interview with DFIR 1, 5 December 2022.
141. *Ibid.*
142. *Ibid.*; views expressed by Counsel 1, November 2022 workshop.

While primarily focused on technical response and recovery,[143] incident responders may also alleviate the harm by providing mental wellbeing support. In part, this comes through the core service provided. This may include providing rapid access to professionals who have experience with ransomware incidents and who offer reassurance to victims.[144] Other interviewees highlighted that some incident response firms had created add-on counselling services for their clients.[145] An incident responder suggested that roughly 20% of clients had taken up a recently formed counselling service, and they confirmed that the service had been well received.[146] This service was 'air-gapped' from the technical incident response activity and was provided by a specialist.

Apart from specialist counselling services, providing ad hoc mental wellbeing support can pose a challenge for incident providers, who are often hired for technical, rather than soft, skills. They often lack counselling qualifications.[147] One interviewee confirmed that 'in crisis management, you're a bit of a grief counsellor'.[148] Another interviewee described that they have worked with emotional clients who – although thankful in the end – were very angry, requiring the team of incident responders to be 'on their tiptoes straight away'.[149] This was reported as being especially the case when victims have a history of mental health difficulties. The success or failure of a business may also be closely entwined with an individual's personal life, as with a micro-SME.[150] In these instances, the incident responder described how they needed to shift to coaching more vulnerable individuals through an issue.[151] In addition, they might help with writing the technical side of ICO reports, improving victims' ability to effectively communicate to the ICO.[152]

Incident responders thus play a critical role in limiting the technical harms that victims experience. However, they can also increase harm where their efforts are unsuccessful. Furthermore, hiring incident responders is often expensive, adding to the financial harm that victims experience. Such costs pose significant challenges for small companies or publicly funded organisations already working with a tight budget, such as schools or local councils.

143. Author interview with DFIR 5, 23 January 2023.
144. Author interview with DFIR 2, 6 December 2022.
145. Author interview with DFIR 6, 1 February 2023.
146. *Ibid.*
147. Author interview with DFIR 5, 23 January 2023.
148. Author interview with DFIR 1, 5 December 2022.
149. Author interview with DFIR 2, 6 December 2022.
150. *Ibid.*
151. *Ibid.*
152. Author interview with DFIR 1, 5 December 2022.

Negotiators

The interview data highlighted that contracted specialist negotiators can be a useful service that improves the experience of the victim organisation. Unlike the victim, who is likely to be in the midst of their first engagement with ransomware operatives, specialist negotiators have extensive experience of communicating with various ransomware operatives. They understand how to approach the operatives to either negotiate a lower ransom payment or acquire as much information from the operatives as possible.[153] Conversely, direct negotiations between the victim and the attacker can introduce additional risk. A negotiator described how the 'worst thing' a victim organisation can do is open discussions with the attackers at an executive level: attackers are likely to exploit this by ratcheting up pressure and insisting on demands for a high ransom.[154] Interviewed ransomware victims noted that their contracted specialist negotiators would typically pretend to be a more junior member of the victim organisation, for example a secretary.[155] This enabled the negotiator to feign technical ignorance and, importantly, insist that they needed to check with superiors before making any decisions or offers, potentially increasing negotiation leverage.[156]

In a trend that may closely mirror the earlier professionalisation of traditional kidnap and ransom services,[157] threat actors likely know they are speaking to contracted specialists, rather than the victims themselves. However, there are still positive aspects of drawing on the services of negotiators. Notwithstanding general increases in the value of demanded cyber ransoms,[158] there are some indications that threat actors and contracted negotiators are normalising a process and dialogue that sees ransoms haggled down by an 'industry standard' of roughly 40%.[159] Contracting negotiation services may therefore lower the ransom payment and overall incident costs. A prominent public example of ransomware negotiation comes from Royal Mail, which succeeded in stalling for time through negotiations.[160] Royal Mail seemingly used the extended timelines to obtain proof of data theft from the criminals in order to implement technical

153. Author interview with Ransomware Specialist 1, 12 December 2022; author interview with Ransomware Specialist 3, 7 March 2023.
154. Author interview with Ransomware Specialist 1, 12 December 2022.
155. *Ibid.*; author interview with Education 1, 8 December 2022.
156. Author interview with Ransomware Specialist 1, 12 December 2022.
157. Anja Shortland, Tom Keatinge and Jamie MacColl, 'Insurance as Crime Governance: Comparing Kidnap for Ransom and Ransomware', *Whitehall Report*, 2-23 (March 2023).
158. Dan Milmo, 'Ransomware Payments Nearly Double in One Year', *The Guardian*, 10 May 2023.
159. Author interview with Ransomware Specialist 1, 12 December 2022.
160. Mark Stockley, 'Royal Mail Schools Lockbit in Leaked Negotiation', Malwarebytes, 23 February 2023, <https://www.malwarebytes.com/blog/news/2023/02/royal-mail-gives-lockbit-a-lesson-in-ransomware-negotiation>, accessed 10 June 2024.

measures that enabled the return of some of its operations by bypassing the encrypted systems.[161]

Specialist negotiators can also provide victims with advice about the ransomware criminals: for example, whether offered decryption keys are likely to be viable, or whether operatives' claims about deletion of exfiltrated data are credible.[162] This provides valuable insight when a victim organisation is seriously considering making a ransom payment. Negotiators can also use their experience to identify irregularities: for example, when the normalised dialogue referred to above is not taking place. A victim described how their negotiating service noticed that their threat actors seemed inexperienced.[163] Thanks to the services of the negotiating firm, the victim organisation was able to exploit the threat actors' inexperience by offering a low-ball payment.

PR Firms and Media Relations Teams

Many victims hire external PR support to ensure good communication throughout the incident and its aftermath. Some interviewees said that external communications services were helpful in guiding external communications and drafting statements. One victim described their communications service as 'excellent'.[164] Others, however, were less content. A victim in the education sector stated that the PR team engaged was not specialised in their sector and was therefore unable to comprehend the needs of a higher education customer.[165]

PR firms are often primarily hired to deal with media relations. Like many engagements with other third parties, interactions with media are a double-edged sword for the victim experience, as they serve as an amplifier of good or bad communications. While some companies, particularly Norsk Hydro, were cited as organisations that benefited from wider media attention,[166] many victims remain sceptical of media reporting and are reluctant to engage with media representatives. One external counsel even spoke about an incident where the company sought 'a complete injunction against any publication of any information concerning the incident, so there could be no media reporting' to ensure there were no reputational consequences.[167] This was regarded among interviewees as a success.

161. Alex Scroxton, 'Royal Mail Refused to Pay £66m LockBit Ransom Demand, Logs Reveal', *Computer Weekly*, 15 February 2023.
162. Author interview with Ransomware Specialist 1, 12 December 2022; author interview with Ransomware Specialist 3, 7 March 2023.
163. Author interview with Technology 3, 24 March 2023.
164. Author interview with Outsourcing 1, 15 December 2022.
165. Author interview with Education 3, 10 January 2023.
166. See, for example, author interview with DFIR 5, 23 January 2023.
167. Author interview with External Counsel 3, 21 December 2022.

Again, it is the fear of further – reputational or other – harm that overshadows victims' perspective on the role of media. One victim referred to a case where media coverage led to additional harm. They explained how, after the incident spread on the news, they experienced a 'massive increase in … general denial of service attacks, people trying to get in the front door'.[168] An insurance expert went as far as saying 'if there's any press interest … , that's never good' – especially for smaller businesses not used to being in the spotlight, as was the case for an individual who had a photographer appear at their house.[169] Further concern related to media coverage causing additional long-term harm, given that once the information is online it often remains publicly accessible long after the incident and can therefore also be read by new clients.[170]

Privately hired third-party service providers therefore significantly impact the victim's experience. They are a powerful factor that can improve the victim experience if the relevant services are provided swiftly and are effective. However, if third-party service providers are unable to provide such positive impact, for example because they are inexperienced in a ransomware setting, fail to deliver adequate technical support, or provide advice that is not tailored to a victim's specific situation, they may significantly contribute to the harm a victim experiences. Policymakers must therefore recognise the key role that private sector services play in the ransomware response and the victim experience. Initiatives setting out recommended incident-response services make it easier for victims to find a service that is more likely to provide services that lessen the harm experienced. Policymakers must also consider how ransomware victims, such as schools or councils, that often cannot afford the response services examined here or might not have cyber insurance, can have access to services that alleviate their harm.

Internal and External Communications

Communications are a critical element determining the victim experience and can either alleviate or aggravate the harm that a ransomware attack causes. Of course, communication can be interrupted on a technical level during an incident, for example because email servers are down or because employees' phone numbers are not accessible. This section does not address these practical concerns but focuses on communications from a strategic perspective.

168. Author interview with Education 3, 10 January 2023.
169. Author interview with Insurance Claims 1, 14 December 2022.
170. Author interview with External Counsel 4, 1 March 2023.

External Communication

External communication is often the main concern of victim organisations, particularly how to communicate with customers or stakeholders, as well as students or parents. Interviews generally pointed to the relevance of sector-specific and context-tailored communications and victims' reluctance to be transparent in their external communications.

Communicating a narrative of victimhood may also have a positive impact. This was the case for a victim in the education sector whose communications team managed communications, including on open social media. There, reactions entailed 'a neutral to positive sentiment', because 'people saw us as a victim, which always helps because people sympathise with victims'.[171] Interviews also highlighted that external communication is particularly challenging for those employees who are not part of the immediate response team. While they might not have comprehensive insights themselves, they are often the ones who must communicate with clients or customers in the aftermath of the incident. One interviewee spoke of 'difficult conversations people had to have with their customers when they weren't allowed to say anything', which they described as 'very stressful'.[172]

To limit their harm, victims must strike the right balance between over- and under-communication. This is a highly context-specific task. On the one hand, a classic mistake is 'over communication and not thought through communication', both to customers as well as in fulfilment of legal notifications.[173] This can actually make the situation worse when the victim who wants to get the message out does not understand the wider implications.[174] Too little communication, on the other hand, can cause additional harm, as the example of the 2023 Capita ransomware attack has demonstrated, where the victim was heavily criticised for insufficient communication.[175] Interview data included a victim in the public sector who regretted not communicating more openly with residents to explain the gravity of the situation in more detail, which in turn led to frustration from their side.[176] Another victim described that they 'were so petrified' that their ransomware attack would be disclosed to clients that they did not communicate openly, instead referring to it as a 'cyber incident'.[177] However, employees were able to correctly guess what the incident entailed. This communication strategy led to a credibility gap, according to the victim.

171. Author interview with Education 1, 8 December 2022.
172. Author interview with Technology 1, 20 March 2023.
173. Author interview with External Counsel 1, 12 December 2022.
174. *Ibid.*
175. Katie Prescott, 'Silence is Deafening After Cyberattack on Capita', *The Times*, 24 April 2023.
176. Author interview with Local Government 2, 1 March 2023.
177. Author interview with Outsourcing 1, 15 December 2022.

Striking the balance between over- and under-communication is often difficult for victims. This is especially the case when operating with limited time to fulfil noticing requirements, or where legal advisers or PR experts are telling them to limit communications and transparency, or when they fear that sharing too much information will result in further harm. This was, for example, the case for an interviewee who described the careful consideration that was needed in communications due to stock market rules.[178] In some instances, even government ministers have told councils not to go public with the incident.[179]

Internal Communication

The interviews stressed that internal communications had an important impact on the victim's experience. Internal communication is a key tool to keep up morale and improve the effectiveness of the response. A victim from the education sector stated that 'keeping people in the loop about what's happening was a key factor in reassuring people that we would come through it'.[180] Interviewees pointed out that internal communication is especially relevant to ensure that those employees who are not part of the inner circle that is responding to the incident are included and aware of what is going on. Likewise, where such communication is weak, they might feel excluded. This led one victim to regret not including earlier those not directly involved, for example by giving them advance notice of when they would be involved again.[181] An interviewee in the technology sector identified the importance of better internal communications as one of their key lessons from the incident.[182]

When internal communication was poor, '[i]t affected morale very quickly', as one victim from the professional services sector explained. For them, internal communications 'were not optimal' as the organisation handled internal questions poorly.[183] In this instance, the poor communication led to 'very worried staff and eventually that became public as well'.[184]

Internal communication includes communications with contracted third parties. It may also require victims to engage with other co-workers with whom they may not ordinarily work. Communicating during the incident can be difficult as it requires engagement with a wide range of stakeholders, varying in technical

178. Author interview with Engineering 1, 10 March 2023.
179. Author interview with Local Government 2, 1 March 2023.
180. Author interview with Education 2, 16 December 2022.
181. Author interview with Education 1, 8 December 2022.
182. Author interview with Technology 1, 20 March 2023.
183. Author interview with Professional Services 1, 17 March 2023.
184. *Ibid.*

expertise and seniority. One victim described 'flipping between different types of conversations' as 'challenging'.[185]

Interviews also addressed challenges communicating technical problems to a non-technical audience. One IT staff member in the charity sector described the difficulties that they experienced in communicating what was happening to senior management whose members lacked technical knowledge. This staff member did not want to undersell the gravity of the situation, but equally did not want to overburden the other party.[186] They also felt there was a risk that senior management could think the IT team was incompetent based on these communications.[187] Similar observations were also true for incident responders, who might also have to brief CEOs of large companies, people with whom they would not normally interact without months of preparation, but now had to brief under considerable pressure.[188]

Similarly, a victim in the financial services sector felt that as boards 'will only talk in money', it was not sufficient to state that their team was performing poorly. Instead, they developed a cost model that described costs incurred – due to ill team members or the need to hire contractors or onboard new staff – to gain the board's attention.[189]

Internal and external communications therefore have a strong influence on the victim experience. Striking the right balance between over- and under-communication can alleviate the victim's harm; failing to do so can aggravate it. While communication strategies are highly context- and victim-specific, policymakers and practitioners must be aware of their potential impact and promote the importance of a good external and internal communication strategy. A strong internal communication strategy is particularly important as it risks being overlooked in current approaches to incident response and planning.

Transparency and Information Sharing

The role of transparency and information sharing was a recurring theme throughout the interviews. The importance of getting good advice from external parties, previous victims or the public sector stood in contrast to the limited transparency and secrecy that occurs in practice. Secrecy about the incident often results from feelings of shame or fear of reputational and subsequent financial harm. However, the advice of third parties such as lawyers and PR

185. Author interview with Education 3, 10 January 2023.
186. Author interview with Charity 1, 12 January 2023.
187. *Ibid.*
188. Author interview with DFIR 2, 6 December 2022.
189. Author interview with Financial Services 1, 9 December 2022.

specialists can make victims even less likely to share their experience. This is the case when they are counselled against sharing too much information as it might be used against the victim in subsequent legal proceedings. Interviewees critically discussed the role of lawyers and legal privilege in this context. While many victims confirmed they were given legal advice not to share information, some experts did not see legal privilege as stopping victims from sharing information in all circumstances. One legal expert stressed that while they cannot share information about individual clients, general comments and anonymised information can nevertheless provide valuable insights on best practice, without legal risks.[190]

The lack of transparency among victims was repeatedly raised during the research for this paper. For example, one victim reported feeling isolated during the incident after they were told not to share their experience.[191] During the interviews, it became evident that victims found it helpful to talk about their experience, either in the interview itself or in other forums they previously explored. One victim stated that they 'found it quite useful just to talk to you and other people, in a candid open approach ... I found that useful, and I think it might help people'.[192] This again links to the limited attention paid to the psychological impact and the individual's experience of a ransomware attack in corporate cultures that provide little opportunity to process the experience.[193]

But it is not just the individual victim that would benefit from greater transparency. More information exchange among victims and potential victims is a meaningful way to share best practices.[194] One victim described the challenging situation that they faced when they wanted to warn a colleague and friend in another education institute, so that they could block IP addresses and take other enhanced security measures. However, legal advice prohibited the victim from sharing this information.[195] Similarly, another victim in the public sector stressed the importance of sharing their experience to raise awareness among other public sector institutions, especially to challenge over-confident assumptions that they would not be impacted by an attack.[196]

Sharing information among victims offers unique insights: for example, as a reminder to others that they will make it through the incident. Victims might also provide recommendations for sector-specific best practices or be able to

190. Author interview with Professional Services 1, 17 March 2023.
191. Author interview with Consultancy 2, 17 March 2023.
192. Author interview with Education 3, 10 January 2023.
193. MacColl et al., 'The Scourge of Ransomware'.
194. This was confirmed, for example, by the interviewee in author interview with Professional Services 1, 17 March 2023.
195. Author interview with Education 3, 10 January 2023.
196. Author interview with Local Government 2, 1 March 2023.

offer empathy on a deeper level. One victim described that they read ransomware reports prior to experiencing an attack themselves. However, it was more of an intellectual exercise, whereas after the incident, reading the reports made them 'feel a lot of sympathy for the companies that are currently trying to navigate their way through these issues'.[197]

While interviewees broadly agreed that greater transparency was desirable, there was little agreement on the mechanisms to share information. Suggestions that government bodies such as the NCSC should encourage greater transparency or set up an exchange platform were met with mixed reactions. Some interviewees pointed out that any institutionalised approach would deter victims from sharing openly. There was a preference for a peer-supported group, but questions remained as to its exact structure and feasibility.[198]

Information sharing to enhance understanding of best practices and the desire for greater transparency among victims therefore stands in contrast to the secrecy that often surrounds ransomware attacks. While the benefits of more information sharing are clear, enabling such practices requires a forum where victims feel safe to share their knowledge.

The Influence of Regulators

Engagements with regulators have a significant impact on the victim experience. In the UK, a ransomware victim ought to report their incident to law enforcement, but they are not obliged to do so.[199] If, however, the ransomware incident has affected personal data, the victim must report it to the ICO within 72 hours of first becoming aware of the event.[200] The ICO safeguards data subjects who are affected by the exposure of their personal data. It is obliged to ensure that organisations – including those on whom ransomware has an impact – comply with mandatory data compliance. Framing the data subject as the victim-to-protect has important implications for interactions between the victim organisation (and its staff, who may also be data subjects), their third-party support and data regulators. This paper therefore does not provide a complete assessment of ICO activities but focuses instead on how ransomware victims perceive the ICO and its work.

In 2022, a third of cyber cases reported to the ICO related to ransomware, possibly creating the most comprehensive database of UK ransomware victims.[201]

197. Author interview with Engineering 1, 10 March 2023.
198. Author interview with Workshop 2, 28 February 2023.
199. Author interview with External Counsel 2, 14 December 2022.
200. ICO, 'Personal Data Breaches: A Guide', <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/>, accessed 10 June 2024.
201. Alexander Martin, 'Ransomware Attacks Hit Record Level in UK, According to Neglected Official Data', *The Record*, 12 September 2023, <https://therecord.media/ransomware-attacks-record-in-UK>, accessed

Interviewees were keen to share their experiences of engaging with the ICO during and after their ransomware incidents. Such engagement was repeatedly identified as a critical factor that aggravated the victim experience.

The overriding complaint made about the 'ICO experience' was the time taken for investigations. A range of factors determine the time taken to investigate. For example, they can include: an organisation's ability to provide information; workloads during the Covid-19 pandemic; or funding models. In some instances, the time needed to engage with the ICO vastly exceeded almost all other remediation aspects of a ransomware event, barring data subject litigation.[202] Another victim expressed frustration that a fresh request for information from the ICO asked 'basic' questions that had already been comprehensively answered in a previous response.[203] The engagement with the ICO was likely to last for months, but could extend to a year or more.[204] An interviewee from an education organisation affected by ransomware noted that their case with the ICO was still ongoing two years after the incident.[205] A legal practitioner with experience of supporting ransomware cases noted that they suspected that funding and/or staffing issues were causing this.[206] Reporting has previously suggested that under-resourcing may be an ongoing issue,[207] although the ICO's annual reports highlight a significant increase in staffing from 2020/21 to 2022/23.[208] Additionally, given that the ransomware victim experiences included in this project's data corpus partially occur at the same time as various Covid-19 restrictions, it is possible that altered working practices contributed to some delays or the perception of delays in processing times.

Nonetheless, the suggested delay in reaching 'closure' from a ransomware event was a source of frustration, stress and upset for victims. Victims referred to a 'Sword of Damocles' effect: they were unsure whether the ICO was going to fine or censure them.[209] The process of engaging with the ICO was also described as laborious. A victim from the education sector, for example, described being

23 February 2024; ICO, 'Data Security Incident Trends', last updated 11 May 2024, <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>, accessed 21 May 2024.

202. Author interview with Insurance Claims 1, 14 December 2022.
203. Author interview with Education 4, 24 October 2022.
204. Author interview with Insurance Claims 1, 14 December 2022; author interview with Local Government 1, 15 December 2022.
205. Author interview with Education 4, 10 March 2023.
206. Author interview with External Counsel 4, 2 March 2023.
207. Bill Goodwin, 'Surrey and Sussex Police Spared Fines after Recording 200,000 Phone Calls Without People's Knowledge', *Computer Weekly*, 19 April 2023; Keumars Afifi-Sabet, 'Understaffed Data Regulators Putting GDPR at Risk of Collapse', *ITPro*, 29 April 2020, <https://www.itpro.com/policy-legislation/general-data-protection-regulation-gdpr/355476/understaffed-data-regulators>, accessed 23 February 2024.
208. ICO, *Information Commissioner's Annual Report and Financial Statements 2019-20*, HC 477 (London: The Stationery Office, 2020); ICO, *Information Commissioner's Annual Report and Financial Statements 2022/23*, HC 1440 (London: The Stationery Office, 2023).
209. Author interview with Outsourcing 1, 15 December 2022.

'bombarded' with letters and felt victimised.[210] A response to ICO letters would beget further letters requesting detailed information from the IT team.[211]

As indicated earlier, the ICO has a mandate to investigate data compliance practices. That said, there was a significant trend: interviewees widely noted that their experience with the ICO added further harm at an already difficult time. For some, the protracted timelines made it difficult for them to move on after other aspects of the incident had already been finalised. However, it must be noted that while most experiences with the ICO were negative, some interviewees reported more positive experiences. For instance, the coordinator of an IT ransomware response at a charity organisation noted that while there was a wait for the ICO response in their case, they felt that the response was supportive and understanding.[212] While the reports and interviews took time, they found the overall experience to be 'less terrifying' than anticipated.[213]

The conduct of those reporting to the ICO may also potentially have a bearing on experiences. An IT director from the education sector noted that they proactively kept the ICO up to date on the investigation and remediation processes; they believed their transparent and forthcoming approach smoothed their engagement with the ICO and facilitated an ideal outcome.[214] A digital forensics and incident response interviewee noted that victim organisations – or those supporting them – need to have a clear picture of what data the organisation holds and which data subjects are affected; if a written response to the ICO did not provide all the information legally required, it was likely that the exchange of letters would be lengthier.[215] The coordinator of an IT response at a multinational engineering firm noted that they sent a courtesy email to the ICO before they notified the stock market of their incident, but that because of the nature of their incident, there was no follow-up or investigation.[216] There were also suggestions that organisations should not rush to make a report to the ICO before they have a clear understanding of what has occurred, and that ideally they should seek guidance from an experienced external counsel before making a submission.[217] A legal practitioner noted that, despite their guidance, it was not uncommon for stakeholders at a client victim organisation to 'panic overnight' in the first day or two of an incident and clumsily report to the ICO, causing additional avoidable

210. Author interview with Education 2, 16 December 2022.
211. *Ibid.*
212. Author interview with Charity 1, 12 January 2023.
213. *Ibid.*
214. Author interview with Education 2, 10 January 2023; author interview with Government Agency 2, 3 March 2023.
215. Author interview with DFIR 7, 21 February 2023.
216. Author interview with Engineering 1, 10 March 2023.
217. Views expressed by Breach Counsel 1, November 2022 workshop.

pain in the ensuing months.[218] This is a tricky balancing act, particularly given the 72-hour deadline for notifying the ICO following awareness of a breach.

Additionally, it should be emphasised that the ICO has an important role in protecting the data rights of UK data subjects. Where a ransomware event impacts data subjects, they too are victims of the ransomware. Interviewees noted that the ICO was a necessary part of the UK's regulatory system and that it was right that it should follow due process and work to drive positive transparency in organisations.[219] Ultimately, the data corpus indicated that there is a balance that should be struck between empathising with organisations that receive a ransom note as victims of serious international organised crime and using regulatory pressure to encourage the adoption of stringent personal data-protection practices.[220] While the purpose of the ICO may be apt, changes that can improve the victim experience may be possible. Those that can, wherever possible, reduce the prolonged stress and uncertainty are especially important. Victims also should not need to resubmit identical evidence or information when a prior comprehensive reply has already taken place. At the same time, victim organisations should be advised that they can submit a brief initial report within the 72-hour limit, and therefore avoid submitting a more detailed report in haste during the opening phase of an extremely stressful crisis situation. Here, the support of experienced external counsel may be particularly useful to coordinate a measured or cautious initial submission.

218. Views expressed by Legal 1, February 2023 workshop.
219. Author interview with Technology 1, 20 March 2023.
220. Author interview with Insurance Claims 1, 14 December 2022.

III. The Role of Government, the NCSC and Law Enforcement

This chapter sets out the role of the public sector support and engagement network ecosystem. Findings are based on interview discussions on the support victims receive from local police, regional organised crime units (ROCUs), the NCSC and the NCA, as well as the engagements victims have with the ICO. The analysis does not cover the capacity of government and law enforcement bodies to bring ransomware operators to justice. Rather, it draws insights on the nature, scale and impact of public sector support for ransomware victims. Specifically, the focus is on the degree to which this support ecosystem improves and/or exacerbates a victim's experiences during a ransomware incident.

Table 3: Types of Support Provided to Ransomware Victims, by Organisation

Victim Support Activity	Local Police	Regional Police	NCA	Action Fraud	NCSC	ICO
Pre-breach guidance	•	•	•		•	•
Assurance of IR services					•	
Pre- or post-breach notification	•	•	•		•	
Forensic intelligence gathering	•	•	•		•	
Assessment of secondary risk exposure	•	•	•		•	
Passive crisis management support	•	•	•		•	
Active crisis management support					•	
Provision of decryptors	•	•	•		•	
Provision of crime number				•		
Review of data protection compliance						•

Source: The authors.

Types of Support

The police, NCA, NCSC and ICO may support ransomware victims in a variety of ways. Table 3 provides an indicative list of support categories. Note, pre- and post-breach notifications may most commonly relate to 'Protect' notifications that law enforcement may issue to organisations after receiving intelligence about a current or likely breach. 'Passive' crisis management support refers to activity such as sitting in on teleconference calls between victim personnel and colleagues from their third-party incident response firm. Conversely, 'active' crisis management refers to on-the-ground remediation support, which may include technical remediation of affected systems. As highlighted in the next section, active crisis management is less commonly provided than its passive equivalent.

How NCSC and Law Enforcement Support is Allocated

The interview data highlighted that the makeup of the support ecosystem is likely to vary depending on the context of an individual victim. The NCSC's cyber incident framework provides an indication, ranging from Category 1 (national cyber emergency) to Category 6 (localised incident).[221] A direct victim experiencing a Category 6 incident is likely to find that their incident is supported by local police. At Category 4 or above, the NCSC may become involved, with a greater likelihood of NCSC coordination/lead at Category 3 and above. As the incident framework articulates, the assessment is, in part, driven by the likely impact of an incident on societal or governmental functions.[222]

In principle, an SME providing a vital service that experienced a disruptive ransomware incident could therefore receive NCSC support.[223] There is a degree of fluidity with the support ecosystem, but this equally leads to a sense of uncertainty as to who can expect NCSC support and under what circumstances. A ransomware victim may find that the level of support aligns with, exceeds or does not meet their expectations. An incident responder described their view that UK law enforcement was 'more hands off … [they're] advising and taking details, and then waiting for the victim to provide additional information at a suitable time'.[224] In some limited cases, victims may be able to draw on NCSC/

221. NCSC, 'Categorising UK Cyber Incidents', 23 August 2023, <https://www.ncsc.gov.uk/information/categorising-uk-cyber-incidents>, accessed 10 June 2024.
222. *Ibid.*
223. Author interview with NCSC 2, 24 February 2023.
224. Author interview with DFIR 3, 12 December 2022.

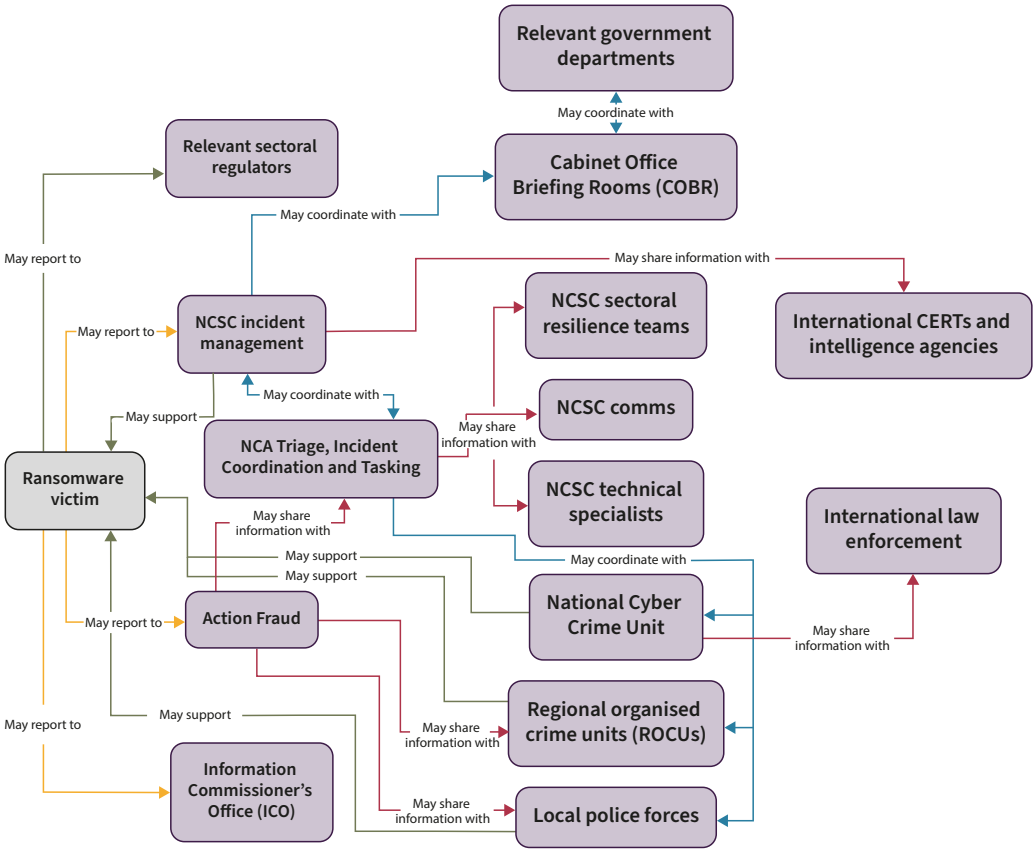
GCHQ technical remediation support,[225] although this service is constrained by resource availability.[226] A government interviewee described how they were not resourced to compete with the private sector, noting that '[Microsoft, Google, Mandiant,] the budgets of these organisations outweigh anything I've got … [our] challenge is to work out how to … sit alongside and complement appropriately what exists out there … we need to be realistic. The national resource is targeted at nationally significant incidents'.[227]

The law enforcement engagement during a typical ransomware victim experience is likely to start with a submission to Action Fraud. Victims who call the national emergency number will probably be redirected to Action Fraud, unless they are particularly high profile.[228] The victim enters text describing the nature of their incident into the Action Fraud submission page. From here, the case is reviewed and triaged; an SME, for example, may be supported by local police, whereas a larger organisation with a regional significance, such as a large university, may be supported by a regional organised crime unit (ROCU).[229] It is also possible for some organisations to be directed to the police after being in contact with the NCA. The victim of ransomware can anticipate that the local or regional police will gather data about the incident, in part to support a regional or national profile of cybercrime trends.[230] The victim may also receive support from law enforcement sources, for example guidance on external communications with stakeholders, or suggestions regarding post-incident 'aftercare', such as vulnerability assessments or cyber exercises.[231] Figure 4 summarises the interactions that are possible.

Processes are not, however, uniform and victim experiences may vary significantly even within a single jurisdiction such as England. On paper, while most victims should contact Action Fraud as a first port of call, there are circumstances where this step may be bypassed. A supplier of critical national infrastructure (CNI), for instance, could bypass Action Fraud altogether and instead report directly to the NCSC.[232] It is also possible that the NCSC and the NCA may draw on intelligence to proactively reach out to a high-significance victim that has avoided

225. Author interview with Local Government 2, 1 March 2023.
226. Author interview with DFIR 5, 23 January 2023.
227. Author interview with NCSC 2, 24 February 2023.
228. Author interview with Law Enforcement 2, 13 December 2022.
229. *Ibid.*
230. *Ibid.*
231. *Ibid.*
232. Author interview with Law Enforcement 1, 9 December 2022.

Figure 4: How UK Ransomware Victims Interact with Public Bodies



Source: The authors.

reporting their incident.[233] The length of time during which a ransomware victim can expect to liaise with law enforcement can also vary significantly, ranging from weeks to months.[234] It is also worth noting that victims of ransomware may also avoid engagement with the NCSC or law enforcement altogether. All ransomware victims interviewed for this project had engaged with law enforcement in some way. This may reflect the bias of voluntary participation research; individuals who were willing to share their experiences with the research team may be more likely to engage with law enforcement. However, wider reporting suggests several reasons for avoiding law enforcement engagement. These include perceived reputational risks and the fear that law enforcement forensics may interfere with a restoration effort.[235] Additionally, victims may fear that law

233. Author interview with Financial Services 1, 9 December 2022.
234. Author interview with Law Enforcement 3, 17 October 2022.
235. Danny Palmer, 'Ransomware Victims Aren't Reporting Attacks to Police. That's Causing a Big Problem', *Zdnet*, 5 October 2020; Joint Committee on the National Security Strategy, 'A Hostage to Fortune: Ransomware and UK National Security', HC 194/HL Paper 23, House of Commons and House of Lords, First Report of Session 2023–24, 13 December 2023.

enforcement, once involved, might find other things of interest beyond the ransomware incident to which they do not want to draw attention.

Given the sensitivity of a ransomware incident and the desire to control external communications, victims may fear that engagement with law enforcement might increase possible negative exposure. This might include, for example, details of the incident appearing in the press. Additionally, the pressure to restore business operations and move on from the incident means that victims may be concerned that law enforcement agencies will want to take copies of impacted sections of an IT estate for forensic investigation, possibly stalling recovery efforts. This latter point – investigation versus recovery – is a potentially important area of contention. The interests of the individual victim organisation (an effective recovery as soon as possible) may run counter to the interests of wider society (understanding the nature of the ransomware threat). Counter-ransomware successes such as the February 2024 NCA-led takedown operation against LockBit benefit from maximum access to intelligence within the UK and among international law enforcement partners.[236] Furthermore, counter-ransomware initiatives may also stem a ransomware group's activity and thereby reduce future harm. Existing and new victims may also benefit from seized decryption keys being shared by law enforcement.[237]

The Impact of Police Support: Perspectives from Victims and Stakeholders

Many interviewees were keen to share their experiences of their interactions with law enforcement services during and after their ransomware incident. Given the nature of the distribution of response – with the NCSC liaising with select cases – victims were much more likely to have experience of dealing with local or regional police. This section draws on insights from victims' assessments of the efficacy of police in dealing with ransomware incidents. The analysis also draws on the perspectives of stakeholders from the ransomware support ecosystem, such as incident responders.

Findings in this section need to be seen in their appropriate context: law enforcement services operate with limited resources, and ransomware victims are likely to be under severe stress during their incidents. With these circumstances

236. National Crime Agency (NCA), 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group', 20 February 2024, <https://www.nationalcrimeagency.gov.uk/news/nca-leads-international-investigation-targeting-worlds-most-harmful-ransomware-group>, accessed 4 March 2024.
237. Alex Hern, 'Seized Ransomware Network LockBit Rewired to Expose Hackers to World', *The Guardian*, 20 February 2024.

in mind, the findings are nevertheless useful for policymakers and law enforcement stakeholders. For example, it may be possible to identify areas where tweaks to law enforcement practices for ransomware incidents may have a substantial positive effect on the typical victim experience. While it may not be possible to bring perpetrators to swift justice, law enforcement plays an important role as a public sector support system for victims, and as a collator of regional and national data on the ransomware threat landscape.

Through the data corpus, negative perceptions about the role of law enforcement were widespread. A victim from a large multinational firm in the engineering sector noted that they 'didn't see the point' of reporting to law enforcement, citing the lack of a valuable return, during a crisis, and the concern that the police would request data for forensics investigations.[238] Nonetheless, they were quick to add that they had proactively given intelligence to the NCSC and the NCA.[239] A victim from a law firm recalled how they spoke with a cyber specialist from the police who appeared knowledgeable and initially suggested that help may be available to restore systems, but this help did not materialise after a follow-up and the victim was left with the perception that they were on 'their own'.[240] The victim cited their cyber insurance as the most valuable source of support.[241]

The director of a micro-SME compared two cases of police engagement: one on the ransomware attack against their business; and the other on the theft of their car.[242] Within days, the car was identified and retrieved by police before it could leave the UK for illicit international resale; but no support was forthcoming for the ransomware incident.[243] Multiple victims from the technology sector relayed their view that the police were ill-equipped and/or unable to support them during their incidents.[244] One noted that, from their particular experience, they were left feeling that the police were not familiar with the terms 'IP address' or 'VPN', indicating a significant lack of expertise.[245] The policing 'skills and resourcing gap' between analogue and digital crime response capability featured prominently in a recent report by the Joint Committee on the National Security Strategy.[246] Additionally, an inspection report had previously identified that ROCUs were competing with one another for a limited pool of skilled personnel.[247]

238. Author interview with Engineering 1, 10 March 2023.
239. *Ibid*.
240. Author interview with Professional Services 1, 17 March 2023.
241. *Ibid*.
242. Author interview with Consultancy 2, 17 March 2023.
243. *Ibid*.
244. Author interview with Technology 1, 20 March 2023; author interview with Technology 2, 21 March 2023; author interview with Technology 3, 24 March 2023.
245. Author interview with Technology 3, 24 March 2023.
246. Joint Committee on the National Security Strategy, 'A Hostage to Fortune'.
247. HMICFRS, 'National Crime Agency Inspection: An Inspection of the National Crime Agency's Relationship with Regional Organised Crime Units', 12 November 2020, <https://assets-hmicfrs.

Interviewees highlighted that, in some instances, the creation of a crime number may be the extent of police engagement or support.[248] While some victims will receive a visit from the police, others will not.[249] Some victims may not receive any follow-up.[250] More generally, it was notable that there is a degree of inconsistency in law enforcement's engagement with ransomware victims. Concerningly, there were indications of a 'postcode lottery'. While caveating that their experience may be anecdotal, an incident responder described how: 'if you are based near Leicester and you report to Action Fraud, it's going to make it to [the] NCA and they are then going to speak to the local constabulary and you're actually going to get some kind of support. But if you're somewhere else, it's way less likely'.[251]

However, not all experiences were negative. A victim from the education sector described their police cyber unit as 'super supportive … they were excellent, absolutely excellent'.[252] An external counsel interviewee noted that while there continued to be a lack of understanding about the nature of the ransomware victim experience – and the needs of an organisation that has been affected by ransomware – there was an increasing 'uptick' in interest among victims to report incidents.[253]

Pre-existing expectations were a critical factor when assessing law enforcement's support. If a victim's expectations were low, they were less likely to be disappointed when significant support was not forthcoming.[254] This speaks to an important point: evaluations of the 'efficacy' of law enforcement's engagement with ransomware victims will depend on their understanding of the capabilities and limitations of the police in dealing with international cybercrime.

Given limited resources, the police cannot serve as public sector incident response for ransomware. Interviews emphasised that the incident response ecosystem is almost entirely run by the private sector.[255] However, the data corpus also highlighted a growing role of the UK police as a collector and disseminator of intelligence about ransomware threats.

The role of police in ransomware response is, however, not necessarily clear to victims. As law enforcement's ransomware threat landscape purview develops, there may be more opportunities to clarify the role and contributions of law

justiceinspectorates.gov.uk/uploads/an-inspection-of-the-national-crime-agencys-relationship-with-regional-organised-crime-units.pdf>, accessed 23 February 2024.

248. Author interview with Charity 1, 12 January 2023; author interview with DFIR 2, 6 December 2022.
249. Author interview with Charity 1, 12 January 2023.
250. Author interview with Law Enforcement 1, 9 December 2022.
251. Author interview with DFIR 4, 14 December 2022; views expressed by Cyber Security 5, February 2023 workshop.
252. Author interview with Education 3, 10 January 2023.
253. Author interview with External Counsel 1, 12 December 2022.
254. Author interview with DFIR 2, 6 December 2022.
255. *Ibid.*; author interview with DFIR 7, 21 February 2023.

enforcement. One way to do so is by reinforcing a positive feedback loop. An incident responder described how their perception had changed; previously, they saw the benefit of client engagement with law enforcement as 'zero', but their view was changing after law enforcement had proactively reached out to some clients to let them know that their IT estate was being maliciously accessed by threat actors.[256] Unfortunately, this occurred after the ransomware payload had already been delivered, but the responder viewed the proactive contact with clients as a positive reinforcement for encouraging future client reporting to law enforcement.[257] A similar experience was shared by an external counsel interviewee, who noted that while most engagements with law enforcement were 'intelligence gathering' exercises, they had personal experience of a 'handful' of cases where the police joined calls and provided updates on the victim's data exfiltration, drawing on dark-web monitoring.[258] This was regarded by the external counsel as a very helpful development.[259]

A law enforcement practitioner noted that, from their experience, ransomware victims typically reported because they 'feel like they should', rather than doing so out of anticipation of in-person support.[260] Another interviewee – a legal practitioner with experience of supporting ransomware victims – highlighted a sense of pragmatism in their approach to engaging with law enforcement. They noted that while they were cautious about the level of information that they would share, there had never been 'any detriment' to their engagement with law enforcement and that they were collectively united in the interest of fighting against ransomware.[261] They suggested there were 'myths' about the role of law enforcement that may be unhelpfully distorting perceptions of what help is or is not available.[262] A positive feedback loop – in cases where victims have previously shared information with law enforcement – would therefore have an impact by showing victims how such information was used and how it contributed to successful law enforcement activities.

The data suggests that context affects whether the extent of law enforcement engagement can aggravate or reduce the negative experiences of ransomware victims. A range of factors may influence this, including the nature of the victim organisation, its location (including at a county level) and the victim's expectations. While some victims may welcome an arm's-length response from law enforcement, others may want more active support, even if this is only an empathetic ear during a time of crisis. This reinforces the utility of an initial phone call or site

256. Author interview with Insurance Claims 3, 3 February 2023.
257. *Ibid.*
258. Author interview with External Counsel 1, 12 December 2022.
259. *Ibid.*
260. Author interview with Law Enforcement 3, 21 December 2022.
261. Author interview with External Counsel 3, 21 December 2022.
262. *Ibid.*

visit from law enforcement, which can be used to understand a victim's needs and provide clarity about expectations.

The Impact of NCSC and NCA Support: Perspectives from Victims and Stakeholders

Interviewees were also keen to share their perspectives on the perceived efficacy of the NCSC and the NCA in relation to the ransomware victim experience. The functions of the NCSC and the NCA are distinct. However, an interesting finding from the data corpus was that victims reported similarities in their experiences of engaging with the two bodies. It was reported that both agencies had roles in background coordination or oversight in certain ransomware incidents. Some ransomware cases drew the support of one agency while others triggered the involvement of both.

On paper, the incident response framework referred to earlier in this paper partially clarifies the trigger points for NCSC and/or NCA involvement: for example, an incident in Categories 1–4 is likely to warrant some form of NCSC involvement.[263] In practice, however, there was confusion about whether a victim can anticipate NCSC or NCA involvement and the degree of support that may be offered. A government workshop participant indicated that this may be intentional: 'if I'm honest, we have used … a degree of ambiguity, and didn't want to be overly prescriptive on who we wouldn't support. Which I totally get can be frustrating, but … the desire on our side was to ensure that nobody ruled themselves out in coming forward'.[264] Sensitivity about supply chains means that exceptions, caveats and reactivity were important in determining who can access higher levels of government support.[265] For example, even when a victim is technically not part of CNI, their unique and important position in a supply chain might warrant NCSC or NCA support, as the impacts may be similar. Flexibility in how cases are triaged is necessary to manage limited resources and capacity. In the National Security Strategy Joint Committee report, it was recommended that the NCSC and the NCA be sufficiently funded to provide full-recovery support for all public sector ransomware victims.[266] However, there may be some apprehension about

263. NCSC, 'Categorising UK Cyber Incidents'.
264. Views expressed by Government 1, February 2023 workshop.
265. *Ibid*.
266. Joint Committee on the National Security Strategy, 'A Hostage to Fortune'.

providing the funding necessary for this level of service, particularly given the costs of competing with private sector incident response salaries.[267]

Some incident responders work with the NCSC and/or the NCA on almost all their cases due to the size of their typical clients.[268] However, other interviewees reported frustration with the ambiguity surrounding the involvement of the two agencies. They urged that more clarity be provided on the circumstances in which the NCSC in particular becomes involved.[269] Again, expectations on the timeline and level of support were important factors. An interviewee from a government body (with a significant societal purview) described how they informed central government immediately after the ransomware took effect, but did not get a response for seven days and brought on board private support.[270] After this time had elapsed and public pressure mounted, NCSC personnel came on-site and worked 12-hour shifts alongside the organisation's IT staff.[271] As a further indication of inconsistent practices, another government body with a significant societal purview received 'boots-on-the-ground' support from the NCA and a large incident response firm, with regular calls also including the NCSC.[272]

A victim from the technology sector noted that their initial impression after engaging with law enforcement was that the NCA would 'own' the coordination of their response throughout the incident, but that, possibly due to resourcing constraints,– the response was, in effect, passed to the local police force.[273] The victim expressed frustration on two fronts: first, the lack of engagement; and second, the lack of clarity about why the NCA withdrew from the case.[274] It was also noted that information sharing with the NCSC and the NCA can feel like a 'one-way street', where agencies absorb threat and incident intelligence but infrequently share feedback or their own intelligence.[275] The NCSC has also been described as 'tactically focused': predominantly interested in the core incident. A victim who kept the NCSC abreast of their incident remediation and shared intelligence thought that it would have been useful for an NCSC representative to have spoken with members of their executive group after the incident.

267. See Ciaran Martin's comments in Alexander Martin, 'UK Cyber Agency Announces Ollie Whitehouse as its First Ever CTO', *The Record*, 1 September 2023, <https://therecord.media/uk-cyber-agency-ollie-whitehouse>, accessed 23 February 2024.
268. Author interview with DFIR 5, 23 January 2023.
269. Author interview with Insurance Claims 1, 14 December 2022; author interview with External Counsel 1, 12 December 2022.
270. Author interview with Local Government 2, 1 March 2023.
271. *Ibid*.
272. Author interview with Local Government 1, 15 December 2022.
273. Author interview with Technology 2, 21 March 2023.
274. *Ibid*.
275. Author interview with DFIR 5, 23 January 2023.

According to them, this would have helped to relay the seriousness of the event to the business's decision-makers.[276]

More positively, both the NCSC and the NCA were reported to be 'trusted parties' when engaging with victims; victims can approach either body without fear that the government body would share information with the ICO or leak information to the press.[277] An interviewee from a victim organisation that has a CNI-related purview spoke highly of the NCSC's role as a trusted coordinating authority and found their role as a single point of contact to be useful.[278] Both the NCA and the NCSC were also able, in some circumstances, to discreetly liaise with international law enforcement to arrange for the takedown of exfiltrated data.[279] The February 2024 NCA-led operation that successfully seized LockBit servers included exfiltrated data (including data from those who had paid ransoms for deletion of exfiltrated data) and more than 1,000 decryption keys earmarked for victims.[280] This publicly announced hack-back was internationally acclaimed.[281]

Additionally, some interviewees specifically appreciated the laissez-faire nature of NCSC engagement, believing that the victim's own IT team and hired expertise were best placed to remediate the ransomware incident and achieve the best outcomes for the organisation.[282] In part, this approach is pragmatic: the NCSC's incident management team is small,[283] and the agency is not able to compete with the private sector, both in terms of capacity and salaries offered to its staff.[284] It was also suggested that as the NCSC is the public-facing element of a signals intelligence agency, it may not be particularly well placed to serve as an emergency service for most incidents.[285] Ultimately, while the NCSC may serve as an actor-of-last-resort in select cases, it cannot take on this function for many victims. Instead, the NCSC was framed as a source of information and guidance for organisations.[286] It offers a wide range of guidance that organisations can draw

276. Author interview with Engineering 1, 10 March 2023.
277. Author interview with DFIR 1, 5 December 2022; author interview with External Counsel 3, 21 December 2022.
278. Author interview with Outsourcing 1, 15 December 2022.
279. Author interview with NCSC 2, 24 February 2023; views expressed by Legal 1, February 2023 workshop.
280. NCA, 'International Investigation Disrupts the World's Most Harmful Cyber Crime Group'.
281. Hern, 'Seized Ransomware Network LockBit Rewired to Expose Hackers to World'; Connor Jones, 'LockBit Leaks Expose Nearly 200 Affiliates and Bespoke Data-stealing Malware', *The Register*, 21 February 2024, <https://www.theregister.com/2024/02/21/lockbit_leaks/>, accessed 23 February 2024.
282. Author interview with Engineering 1, 10 March 2023.
283. Author interview with DFIR 5, 23 January 2023.
284. Author interview with DFIR 7, 21 February 2023; author interview with NCSC 2, 24 February 2023.
285. Author interview with Technology 2, 21 March 2023.
286. Author interview with NCSC 2, 24 February 2023.

on, before and after an incident.[287] This guidance generally received praise from interviewees.[288]

As noted, the data indicates that, broadly, the NCSC and the NCA have built reputations as trusted partners in coordinating ransomware incidents, particularly those that have a significant societal impact. Interviewees were also generally understanding of the resource constraints that the NCSC and the NCA face and that their active involvement in an incident remediation process must be rationed. This may temper expectations. There were, however, notable exceptions. Some victims felt that they should have received more active government support during their incident. This was particularly prominent in the education sector,[289] which is not included in the UK government's list of 13 CNI sectors.[290] This may reflect a grey area between organisations that feel that they have a societally significant role, but which, according to the data, may not qualify for support. At the same time, ambiguity from the NCSC and the NCA may serve a useful purpose. How these considerations are balanced should be guided by the goal of minimising harms.

As noted in this chapter, the influence of law enforcement on the victim experience reflects the fact that the enforcement 'lag' is incorporated. There are significant structural and judicial impediments to law enforcement's capacity to bring most ransomware operators to justice. However, law enforcement and regulators can play a role in either alleviating or exacerbating the ransomware victim experience. This chapter has identified a range of practices that can either improve or worsen the victim experience across the full timeline of a ransomware incident. This analysis recognises key nuances and the important role of the wider context. However, the analysis also highlighted important areas of divergence in support between, for example, different police forces. The NCSC's informal policy of remaining ambiguous about the circumstances that attract its involvement may warrant refinement over time. Additionally, expectation management, clarity of communication and the use of feedback loops appear to be common underlying challenges.

287. NCSC, 'Advice and Guidance', <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>, accessed 10 June 2024; NCSC, 'A Guide to Ransomware', <https://www.ncsc.gov.uk/ransomware/home>, accessed 10 June 2024.
288. Author interview with Insurance Claims 3, 3 February 2023; author interview with External Counsel 3, 21 December 2022.
289. For example, as expressed in author interview with Education 2, 16 December 2022.
290. Cabinet Office, 'Public Summary of Sector Security and Resilience Plans', policy paper, 2017, <https://www.gov.uk/government/publications/sector-security-and-resilience-plans-2017-summary>, accessed 10 June 2024; National Protective Security Authority, 'Critical National Infrastructure', last updated 25 April 2023, <https://www.npsa.gov.uk/critical-national-infrastructure-0>, accessed 10 June 2024.

Conclusion and Recommendations

Ransomware incidents are deliberately designed to be high-impact events for victim organisations and their personnel. The criminals who code and deploy ransomware seek to cause calibrated harm – or the threat of imminent future harm – against their victims to encourage the payment of a ransom. Whether an attack comes in the form of an encryption or exfiltration event, or both, the attackers exploit an organisation's reliance on its data and data systems. While a ransomware event is invariably a negative experience for victims, a range of factors can make it relatively 'better' or 'worse'.

Drawing on original semi-structured interviews with ransomware victims and expert stakeholders who work with ransomware victims, this paper has identified a range of factors that can influence how harms are experienced. These include factors that are internal to the organisation, such as the level of preparedness and the organisational culture before and after the incident, as well as decisions that are made during the crisis and recovery phases. The overall influencing factors also include those that are external to the organisation, for example, the behaviour of the ransomware threat actors. As the paper has identified, additional external factors include the role(s) performed by third parties such as incident response services, lawyers and public entities (including law enforcement and regulators).

Obviously, prevention of the incident is the optimal outcome. However, ransomware is very prevalent and can have a severe impact for any organisation. It is, therefore, necessary to also focus on 'resilience': the ability to reduce impact and maximise recovery after a breach.[291] This paper's analysis of the internal and external factors may be used to inform ongoing efforts to increase organisational resilience against ransomware breaches.

Drawing on the analysis and findings, the paper proposes a range of cross-stakeholder recommendations that are based on the combined findings of this paper and an earlier RUSI paper on ransomware harms. That paper categorised first-, second- and third-order harms from ransomware incidents.[292] This paper draws on the same original interview and workshop data corpus that informed the first paper. These recommendations focus on ways to alleviate the victim's

291. NCSC, 'Mitigating Malware and Ransomware Attacks', <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>, accessed 10 June 2024.
292. MacColl et al., 'The Scourge of Ransomware'.

harm. To acknowledge the range of actors who can take measures to mitigate victims' harms, these recommendations provide suggestions to victim organisations, third-party service providers and policymakers.

Recommendations for Victims and Victim Organisations

Recommendation 1: (Potential) victims, including those who do not think they will become a victim of a ransomware attack, must continue to improve cyber-specific incident preparation and general cyber hygiene measures.

- *All organisations must consider themselves potential victims of ransomware attacks and must therefore continue to improve their cyber security and cyber hygiene measures.*

  Despite continued awareness campaigns, cyber security is still, all too often, a low priority for many organisations. This is especially the case for public service providers such as schools, and small and micro-businesses. The interview data has shown that good cyber hygiene and cyber security measures can significantly alleviate the harm victims experience. These include good data hygiene and an awareness that any organisation can become the victim of a ransomware attack.

- *Organisations should develop cyber-specific contingency plans to prepare for a potential attack and run simulations of cyber incidents.*

  The interview data has further confirmed that while some organisations have contingency plans, they are largely irrelevant or unsuitable if they are not cyber specific. Cyber-specific incident preparation can also include running exercises simulating a ransomware or other cyber incident.

Recommendation 2: (Potential) victims who are preparing for and responding to a ransomware incident must recognise the importance of mitigating the psychological impact of ransomware attacks.

Psychological impacts affect victims in various ways. They are often overlooked, both in the public discourse and among organisations that fall victim to a ransomware attack. Underlying health conditions and the exact role an individual plays within an organisation's ransomware response can significantly influence their exposure to harm.

- *When preparing for an incident, organisations and cyber security professionals must identify and implement measures to mitigate the psychological impact on individuals directly or indirectly affected by the ransomware attack.*

  This includes 'soft' measures such as normalising discussions about the impact of workload and stress on mental health, as well as cultivating a supportive workplace culture. It also includes specific plans such as budgeting for mental health support and creating rotating schedules and a division of labour to avoid over-reliance on select individuals. Preparation must also view ransomware response as a marathon, not a sprint, and resources must be allocated carefully. Understandably, even with preparation, victim organisations may not necessarily be accustomed to the toll of ransomware incidents. Here, experienced external support can be instructive. Stakeholders in the incident response ecosystem can proactively offer bespoke pastoral support to personnel at victim organisations. As highlighted in this paper, there is anecdotal evidence that some incident response firms are offering a separate confidential service to clients to meet this need.

- *During incident response, measures must be taken to avoid burnout and systematic overwork of individuals. Offering opportunities for victims to talk about their experience can further mitigate the impact of psychological harm.*

  Line managers should be sensitive to colleagues' workloads and the psychological, physical and other harm the ransomware attack has on both the organisation and its staff members. While a ransomware incident will always remain an exceptionally stressful period for a victim organisation, flexibility is required to adjust to staff members' mental health. Special attention needs to be paid to members of core IT teams, whose pivotal role in the technical elements of the initial remediation and the workload (and responsibility) they have during the incident exposes them to aggravating factors. This is set out in greater detail in the first of RUSI's two papers. When over-reliance is unavoidable, annual leave or discretionary time off should be considered, once an immediate crisis period ends. A victim organisation can further offer counselling or therapy for affected staff or, at the minimum, an informal place to talk about their experience.

- *When reflecting on the lessons learned after an incident, senior management must acknowledge the personal implications of the ransomware attack and should communicate this within their organisations.*

  Staff members are aware that a ransomware incident is a moment of crisis and, as such, any response has its flaws. However, several interviewees indicated that they were not looking to senior management for silver-bullet

solutions. Instead, they wanted an acknowledgement of the personal implications that the ransomware attack had for them. For example, one internal report mentioned during the interviews included a post-incident analysis that focused on the financial impact the ransomware attack had on the organisation. It did not, however, speak of the personal toll it caused and the personal dedication and sacrifices it demanded of employees responding to the attack. Acknowledgment of how personally the attack is felt by staff members is a relatively easy, but meaningful, step that senior management and line managers can take to mitigate frustration and ensure good morale among their colleagues.

Recommendation 3: Victims should try to turn their experience into a lesson learned for others and, where possible, communicate with other victims or potential victims in their ecosystem. This can help with personal closure and to raise awareness.

The research for this paper confirms that, for many victims, a ransomware incident is a stressful and potentially dark period in their life, making it hard to talk about their experience. However, the data has also demonstrated the value of talking about the experience, whether it is for personal closure or to provide critical insights to members of their ecosystem and sector to help them better prepare for a ransomware attack. Close communication with lawyers, PR advisers and senior management can help victims gain confidence in making decisions on the kind of information they can share. Victims can also signal their willingness to engage with other victims to their third-party service providers. This would allow such providers to act as networkers for those victims in the midst of a ransomware incident so that they gain the benefit of previous victims' insights. Finally, regional or sectoral organisations, such as business associations, can offer platforms for victims to meaningfully connect or speak to their peers, providing valuable insights and contributing to raising awareness.

Recommendation 4: Victims should realise the importance of reaching the right balance of discretion and transparency within their external and internal communications.

The research for this paper has demonstrated how the right amount of communication and transparency can have a positive impact on the victim experience. It has also underlined that ransomware attacks occur in unique circumstances and that their impact has substantial personal impact. Given the features of each case, it is not possible to provide general advice for victims on how to run their (external) communications during and after a ransomware attack. A victim's external communication strategy is a highly context-dependent balancing act that seeks to avoid both under- and over-communication.

Nonetheless, the research has clearly stressed the importance of an internal communication strategy. Many victims, however, prioritise or only focus on external communication strategies. To retain morale within the affected organisation and to ensure that the staff members not directly working on the ransomware response do not feel left out, victims should establish regular and transparent communication with the wider organisation. This includes a recognition of the personal toll the ransomware incident has for many staff members (see above).

Recommendations for Private Sector Service Providers

Recommendation 5: Third-party service providers must recognise the importance of efforts that mitigate the psychological impact of ransomware attacks and these must form part of their technical, legal or other services to improve victims' experience.

- *Third-party service providers must understand the central role of psychological harm in the victim experience and adjust their performance to consider the individual and psychological needs of a victim.*

  Third-party service providers, such as incident responders and lawyers, offer highly specialised support to victims. While they may excel in their respective disciplines, they are often insufficiently trained in navigating communications with victims going through such a stressful incident for the first time. Organisations offering these services should provide training for their staff on how to offer both professional services as well as communicate in a considerate way to victims.

- *Cyber insurance policies should provide coverage for mental health counselling during and after incidents, and insurers should add recommended counselling services to their panels of pre-approved vendors.*

  Third-party service providers cannot and should not be expected to offer counselling that goes beyond their professional obligations or capability. Instead, service providers such as incident responders should consider recruiting specific staff for their soft social skills, possibly including bespoke counselling staff, therapists, councillors and social workers who can support victims in additional ways.

Recommendation 6: With the consent of the clients, third-party service providers should actively enable information sharing between past, current and potential victims through their networks.

- *Third-party service providers should use their networks to actively encourage victims to share their experience with current and potential victims.*

  Third-party service providers see a large number of ransomware incidents unfold. This makes them highly experienced and puts them in a great position to network between past, current and potential victims. However, it can also mean that what might seem like a uniquely challenging situation to a first-time victim might be the bread and butter of a third-party service provider. Such providers should therefore encourage current and potential victims to talk to former victims who can offer peer insights from the perspective of someone who has gone through similar situations, providing empathetic and tailored support. This is a unique perspective that third-party service providers cannot offer: while they might have worked on many cases, they typically have not been a victim themselves. The research for this paper indicates that many members of the ransomware ecosystem rated these informal transparency and information sharing measures as highly impactful.

- *When providing advice to victims on the degree of information sharing they can conduct, third-party service providers should not just take into account the interests of the victim organisation, such as mitigating legal or reputational risks. Instead, they should balance them against the psychological impacts on victims that might occur by preventing transparency.*

  There are instances when service providers have good reasons to advise a victim to restrict their information sharing or the degree of transparency in communications about their situation to external parties. However, interviews have illuminated that such advice might drive victims into isolation even though they often benefit from sharing their experience. Assessments of third-party service providers differed on whether restricting information sharing – and to what extent – is necessary, with some pointing out that general information sharing is not a problem from a legal perspective. Third-party service providers should therefore carefully balance their advice given to victims on restricting information sharing, taking into account not just the interests of the victim organisation as a whole (such as reputational or legal risks) but also the impact such advice can have on affected staff members and their mental wellbeing. A constructive approach finding a context-specific, carefully balanced solution is needed.

Recommendations for Policymakers and Public Institutions

Recommendation 7: Public policy on ransomware must centre on measures that mitigate victims' harm. This includes acknowledging and mitigating the psychological impact on victims.

- *Any guidance that is shared on how to prepare for, manage and respond to a ransomware attack must include best practices for mitigating the psychological harm, such as managing burnout and stress, as well as offering counselling services where appropriate.*

  The NCSC's guidance on incident management293 or identifying relevant teams and roles supporting incident management,294 for example, do not include specific reference to softer measures to be taken to improve the victim's experience and mitigate psychological impact. The NCSC has targeted guidance on 'putting staff welfare at the heart of incident response'.295 However, greater value is achieved when mental health considerations are woven into guidance on preparation and incident-response plans at all levels. This would serve an important function in protecting IT teams and incident responders from adverse mental health impacts, as well as promote awareness and/or recognition from the board and colleagues.

- *More public funding is needed for further free mental health services, including therapy tailored to individuals affected by ransomware.*

  While some public funding for counselling and therapy is already available, long waiting lists for mental health support indicate that demand is significantly higher than supply. The Action Fraud website refers to victim support provided by the charity Victim Support, primarily funded by the Police and Crime Commissioners, which now includes specific guidance for cybercrime victims[296] and freely provides victim support tools and services, such as helplines and online tools and practices.[297] Enquiries further found that the way to access victim support remained unclear and that gaps in its

293. NCSC, 'Incident Management'.
294. See 'Build: A Cyber Security Incident Response Team (CSIRT)' in *ibid.*
295. NCSC, 'Putting Staff Welfare at the Heart of Incident Response', May 2022, <https://www.ncsc.gov.uk/guidance/putting-staff-welfare-at-the-heart-of-incident-response>, accessed 10 June 2024.
296. Victim Support, 'Cybercrime and Online Fraud', <https://www.victimsupport.org.uk/crime-info/types-crime/cyber-crime/>, accessed 20 June 2024.
297. Victim Support, 'Welcome to My Support Space', <https://www.mysupportspace.org.uk/moj>, accessed 10 June 2024.

provision led to 'loss of trust between victims and the systems in place'.[298] While these findings related to fraud, the authors have found that they are also true for a ransomware context.

Recommendation 8: Public guidance to prepare and respond to an incident is already available and helpful, but must be easier to filter, including for quality.

- *Improve search functions of the NCSC list of guides.*

  Increased awareness, further research and wider coverage of ransomware incidents over the past few years has led to an extensive, yet decentralised, repository of publicly available information, for example in the form of statistics and advice on best practices. This is generally laudable, especially when sources provide practical information that is widely and freely available. There is now a need to filter this information in a central dataset.[299]

  While many interviewees were aware of the NCSC's guidance and commended its utility for ransomware preparedness and recovery, interviewees also found that it is generally difficult to filter for relevant information online, including within the NCSC repository of guides. For example, it might be more intuitive for victims to filter information according to 'before', 'during' and 'after' the incident than it may be to filter for certain authors.

- *Establish a 'Guide of Guides'*

  Interviewees and workshop participants discussed the option of a 'guide of guides' as a centralised repository including both NCSC-approved and NCSC-issued information. This would allow users to rely on a wider range of sources and to filter relevant information, for example, according to sector-specific advice. A 'guide of guides' would also filter advice in advance of an attack, during an incident or on the ransomware landscape more generally.

Recommendation 9: Policymakers need to encourage transparency and information exchange by setting up informal safe space forums.

Despite awareness campaigns about reporting incidents and information sharing, a lack of exchange and transparency still dominates the victim experience. This is highly regrettable, not just from a data-gathering perspective. Further transparency could not only improve statistics and insights into ransomware attacks but also improve the victim experience. When victims share their experience, potential victims can learn from their

298. Fraud Act 2006 and Digital Fraud Committee, 'Fighting Fraud: Breaking the Chain', HL Paper 87, House of Lords, Report of Session 2022–23, para. 378.
299. Author interview with Charity 1, 12 January 2023.

best practices and avoid their mistakes. Additionally, victims may also feel less isolated and may mentally benefit from sharing the information.

- *As a well-connected entity, the NCSC must continue to act as an informal networker between past and potential victims and must encourage transparency and information sharing among a wide range of stakeholders.*

  In practice, victims are not incentivised to be transparent. This is especially the case in official or highly formal channels, as concerns over reputational harm or legal consequences outweigh the incentives to openly contribute to knowledge exchange. To counter these concerns, policymakers should encourage informal safe spaces where victims can anonymously share threat intelligence, best practices and other advice. The status of the NCSC as a 'trusted partner' may support it as a coordinator of feed-forward forums.

- *Greater promotion and expansion of NCSC trust groups is needed, and greater informality should be encouraged.*

  While some trust groups for specific sectors are already convened under the NCSC, victims were largely unaware of them. Furthermore, it is challenging for policymakers to encourage informal transparency as efforts will likely be seen as formal places for information sharing, making victims fear that any information may be leaked or used against them.

Recommendation 10: Establish a positive feedback loop that shares success stories and notifies victims where the information they shared is successfully used for intelligence and law enforcement activities.

To increase transparency and reporting to the NCSC and law enforcement, policymakers should also focus on developing a positive feedback loop with victims that report. This should include sharing success stories of law enforcement activity directly with victims to illustrate their contributions. For example, where a victim organisation has contributed data that leads to a successful arrest, reclamation of ransom payments or prevention of further ransomware breaches against other organisations, this should be shared with the organisation in question to provide closure and endorsement, notwithstanding necessary redactions or anonymisation. Equally, where law enforcement and other public agencies manage to successfully disrupt cybercriminals, greater publicity of these success stories would further encourage support and enhance the reputation of law enforcement, generating further support and trust from wider society.

Recommendation 11: Government authorities need to clarify the tasks of relevant public institutions and their role in the ransomware response.

- *The NCSC should provide more clarity on when and how it can support victims.*

  The ransomware response ecosystem is complex and involves many actors from the public and private sectors. However, the interview data illustrated that such engagement is often challenging for victims, who are uncertain where to turn for assistance, to which organisations they should report incidents and what support they can expect from authorities, and how they interact with one another. Duplication of efforts when engaging with authorities often comes at a time of extreme stress for victims, who have little incentive to engage with authorities when they do not expect anything in return. Greater transparency on the relevant actors, the support they provide and coordination among different authorities would streamline communication efforts, manage expectations for engagements and, ultimately, encourage victims to report and provide information to public authorities.

- *Additionally, the NCSC may consider providing tangible (if hypothetical) examples about differing organisations in various ransomware or cyber breach scenarios, identifying which ones would receive what support, and why.*

  While the public perception of the NCSC's coordination role on ransomware is generally positive, the lack of transparency on the trigger points for NCSC support was criticised. Some ambiguity about the NCSC's exact involvement may be desirable to maintain the flexibility to adjust to certain incidents or allocate resources more freely. But such ambiguity must be balanced against the need for expectation management and to avoid reputational damage to the NCSC. It is particularly important for the NCSC to set out its role in incident response and what it considers when deciding on whether to get involved in a given incident either directly or as a coordinator. Furthermore, victims require clarification on what kind of support they can expect from the NCSC. Better expectation management in relation to victims and the wider public ensures credibility of the NCSC and encourages victims to report their ransomware incident.

Recommendation 12: Police must assume their important role as an accessible face of authority in the ransomware response ecosystem, even where their ability to act is limited.

Lack of resources and training currently makes local police units ill-equipped to contribute to responses. While it is unrealistic to expect law enforcement to provide emergency service technical response, it is nonetheless the case that local or regional police units provide the face of public authority for

victims of ransomware. The experience, detailed earlier in this paper, of the micro-business director whose vehicle was stolen after their ransomware incident, was telling. The exceedingly efficient response to the 'analogue' or traditional crime was juxtaposed starkly against the immaterial response to the ransomware incident.[300]

- *Victims of a serious ransomware breach must be offered telephone and/or on-site contact from a law enforcement body within a reasonable timeframe of the victim's initial report to Action Fraud.*

  The interview and workshop data highlighted a wide disparity in the experience of ransomware victims, with indications that there may be a de facto 'postcode lottery'. In some instances, ransomware victims have seemingly been given a disservice: for instance, when they reported a ransomware incident through Action Fraud but were never contacted by police. Arguably, all genuine ransomware cases should prompt a call and/or offer of a site visit from the police. The ransomware victims interviewed for this project felt – passionately – that they were undeserved victims of serious transnational organised crime. Additional distress was often caused by the fact that the attackers were perceived as remote and 'faceless'. Local or regional police do not need to be faceless. When offered, a perceptible presence or gesture from local or regional police provides victims with a form of recognition of the crime that they have experienced.

  This is not only about public relations; it is an important step in improving the feedback loop. Whether the initial contact with police is positive or negative has an important bearing on the likelihood that a victim engages further with local or regional police during and after an incident. Ongoing or intermittent engagement enables greater opportunities for information to flow in both directions.

Recommendation 13: The ICO should continue to work towards timely assessments of ransomware breaches to avoid further harm to victims.

One of the most prominent 'long-tail' negative experiences cited by ransomware victims was their ongoing engagement with the ICO. Victims routinely engaged in an ongoing exchange of letters with the ICO for months or years after the core elements of their ransomware recovery were complete. As previously noted, the ICO provides a vital service in overseeing compliance with data protection regulations, with a focus on protection of individuals' personal data. Given the potential scale and depth of data exposure implicated by a ransomware event, it is important that the ICO scrutinises organisations.

300. Author interview with Consultancy 2, 17 March 2023.

However, there may be a balance to be struck between the promotion of regulatory compliance and exacerbating a (possible) crisis situation for the ransomed organisation.

- *The resourcing of the ICO should continue to be assessed, to maximise the efficient triage, assessment and completion of investigations, enabling timely closure and/or accountability for organisations.*

The authors of this paper do not determine where this balance lies. However, organisations that were victims of ransomware spoke firmly of their negative experiences of engagement with the ICO. Given that the ICO follows a mandate outlined in legislation, this suggests that legislators may want to reflect on whether the ICO's approach to censuring victims of cybercrime strikes the correct balance. Additionally, the data corpus highlighted instances when stress was unnecessarily and avoidably exacerbated for ransomware victims. This was the case for a victim who was asked questions that had already been comprehensively responded to in a previous written response. If staffing or process issues contribute to such errors, stakeholders may need to consider whether the funding arrangements for the ICO are adequate to meet its task.[301] It should be noted that the ICO has acknowledged the scale of this challenge and has outlined its ongoing efforts to meet it.[302]

301. ICO, 'How We Are Funded', <https://ico.org.uk/about-the-ico/who-we-are/how-we-are-funded/>, accessed 10 June 2024.
302. For example, see ICO, 'John Edwards' Speech Introducing ICO25', 14 July 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/john-edwards-speech-introducing-ico25/>, accessed 21 May 2024; ICO, 'John Edwards' Opening Speech at DPPC 2022', 19 July 2022, <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/07/john-edwards-opening-speech-at-dppc-2022/>, accessed 21 May 2024.

About the Authors

Pia Hüsch is a Research Fellow in the Cyber team at RUSI, focusing on cyber, technology and national security. Her research focuses on the impact, societal risks and lawfulness of cyber operations and the geopolitical and national security implications of disruptive technologies such as AI. Prior to joining RUSI, Pia conducted her doctoral research on the lawfulness of low-intensity offensive cyber operations in international law. Pia has a PhD and an LLM in International Law and Security (with distinction) from the University of Glasgow and an LLB in European Law from Maastricht University.

Gareth Mott is a Research Fellow in the Cyber team at RUSI. His research interests include governance and cyberspace, the challenges (and promises) of peer-to-peer technologies, developments in the cyber risk landscape, and the evolution of cyber security strategies at micro and macro levels.

Jamie MacColl is a Research Fellow in cyber security at RUSI. His current research interests include ransomware, the UK's approach to offensive cyber operations, cyber insurance and the role of private companies in global cyber governance. He has led a range of public and private projects for RUSI, with a particular focus on UK cyber policy. He is also currently a Senior Research Associate at the European Cyber Conflict Research Initiative and a Project Fellow at the Research Institute for Sociotechnical Cyber Security. Prior to joining RUSI, he worked in cyber threat intelligence, where he provided strategic and operational intelligence analysis on the cyber threat landscape. Jamie has an MPhil in International Relations and Politics from the University of Cambridge, where his research focused on UK policy towards Russia since the end of the Cold War. He also has a BA in War Studies from King's College London, where he was awarded the Sir Michael Howard Excellence Award in 2016 and 2018.

Jason R C Nurse is a Reader in Cyber Security in the Institute of Cyber Security for Society and the School of Computing at the University of Kent. He is also an Associate Fellow at RUSI, Visiting Fellow in Defence and Security at Cranfield University, and Research Member of Wolfson College, University of Oxford. He received his PhD from the University of Warwick. Jason's research interests include cyber resilience, cyber harms, ransomware, cyber insurance, security culture, and corporate communications and cyber security. He was selected as a 'Rising Star' for his research into cyber security, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Jason is a professional member of the British Computing Society. His research has been featured in national and

international media including the BBC, *Newsweek*, Associated Press, *The Wall Street Journal* and *Wired*.

James Sullivan is the Director of the Cyber research team at RUSI. He founded and has grown a research group at RUSI that considers a number of themes, including the role of national cyber strategies, the cyber threat landscape, cyber security and risk management, offensive cyber, cyber statecraft and diplomacy, and ransomware. James joined RUSI from Deloitte's Cyber Risk team, where he provided analysis on the cyber threat landscape and advised on defensive measures and risk management strategies. Prior to this, James worked at the National Crime Agency as an Intelligence Analyst specialising in cybercrime threats. James has contributed to a variety of publications and media outlets such as the *Financial Times*, the BBC and CNN, and has provided private briefings on aspects of the cyber threat to high-level forums such as the G7.

Sarah Turner has a PhD in Computer Science from the School of Computing at the University of Kent, as a member of the Institute for Cyber Security for Society. Her research focuses on how families address the cyber security issues arising from using Internet of Things devices in the home. Sarah also has an MPA in Digital Technology and Public Policy from UCL's Department of Science, Technology, Engineering and Public Policy. She has also worked as a researcher at PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity, the UCL Knowledge Lab and 5Rights Foundation on various aspects of socio-technical cyber security and data protection.

Nandita Pattnaik is a member of the Institute of Cyber Security for Society at the University of Kent and has a PhD in Computer Science. Blending 25 years of experience in academia and the IT sector across the UK, Oman and India, Nandita works on the security dynamics of a connected home environment. Her research interests include cyber security and privacy perspectives of users in multi-user homes with multiple devices, insider threats in multi-user homes, the use of online data to understand the security and privacy perspectives of home users, and the effects of cyber incidents such as ransomware on individuals. Nandita has a degree in Analytical Economics from Utkal University and a BSc in Computer Science from the Open University.