RUSI

University of Kent

supported by National Cyber Security Centre

RISCS

Occasional Paper

The Scourge of Ransomware

Victim Insights on Harms to Individuals, Organisations and Society

Jamie MacColl, Pia Hüsch, Gareth Mott, James Sullivan, Jason R C Nurse, 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.

The views expressed in this publication are those of the authors, and do not reflect the views of RUSI or any other institution.

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

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

Cover Image: Nawadoln Siributr / 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

Acknowledgements

The authors are grateful to the UK's National Cyber Security Centre (NCSC) and the Research Institute for Sociotechnical Cyber Security for providing funding for this paper and for their support throughout the research process.

A great deal of thanks must go to the team that helped to guide and shape the paper. Hugh Oberlander, Dina Mansour-Ille, Katharine Fletcher, Edward Mortimer, Louise Chan and Sarah Hudson all provided valuable support and editing. A special thank you goes to Keenan Jones for his contribution to the early stages of the research.

Thanks also go to the peer reviewers, as well as to the various individuals from government and the insurance industry who provided insightful feedback on different stages of the paper and the recommendations.

A final thank you goes to all the participants in this research, particularly individuals who work for organisations victimised by ransomware.

Disclaimer: Any NCSC, law enforcement or other public body personnel interviewed in support of this project **have not**, at any time, disclosed any victim identities or victim-specific information for this project or publication.

Executive Summary

- Ransomware incidents remain a scourge on UK society. Based on interviews with victims and incident responders, this paper outlines the harm ransomware causes to organisations, individuals, the UK economy, national security and wider society.
- The research reveals a wide range of harms caused by ransomware, including physical, financial, reputational, psychological and social harms.
- We set out a framework of:
    - **First-order harms**: Harms to any organisation and their staff directly targeted by a ransomware operation.
    - **Second-order harms**: Harms to any organisation or individuals that are indirectly affected by a ransomware incident.
    - **Third-order harms**: The cumulative effect of ransomware incidents on wider society, the economy and national security.
- Building on an existing taxonomy of cyber harms,[1] this framework will enable policymakers, practitioners and researchers to categorise more case studies on ransomware incidents and to better explain new and existing types of harm to the UK and other countries.
- Ransomware is a risk for organisations of all sizes. The findings from this paper highlight that ransomware can create significant financial costs and losses for organisations, which in some cases can threaten their very existence. Ransomware can also create reputational harm for businesses that rely on continuous operations or hold very sensitive data – although customers and the general public can be more forgiving than some victims believe.
- The harms from ransomware go beyond financial and reputational costs for organisations. Interviews with victims and incident responders revealed that ransomware creates physical and psychological harms for individuals and groups, including members of staff, healthcare patients and schoolchildren.
- Ransomware can ruin lives. Incidents highlighted in this paper have caused individuals to lose their jobs, evoked feelings of shame and self-blame, extended to private and family life, and contributed to serious health issues.
- The harm and cumulative effects caused by ransomware attacks have implications for wider society and national security, including supply chain disruption, a loss of trust in law enforcement, reduced faith in public services,

[1] Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* (Vol. 4, Issue 1, October 2018), pp. 1–15.

and the normalisation of cybercrime. Ransomware also creates a strategic advantage for the hostile states harbouring the cyber-criminals who conduct such operations.

- Downstream harm to individuals from ransomware is more severe when attacks encrypt IT infrastructure, rather than steal and leak data. There is no evidence from this research that the ransomware ecosystem is exploiting stolen or leaked personal data in a systemic way for fraud or other financially motivated cybercrimes. At present, exploiting stolen data for other activities is less profitable than extortion-based crime that takes away victims' access to their systems and data. This finding may inform victim decision-making on when they should and should not consider paying a ransom demand.
- The next paper from this project will outline what kinds of measures can reduce or mitigate many of the harms described in this paper.

Introduction

The UK's National Cyber Security Centre (NCSC) recently assessed that ransomware remains one of the most acute cyber threats facing the UK.[2] In 2023 alone, companies and public bodies affected by ransomware incidents in the UK included the Royal Mail, outsourcing firm Capita and an NHS trust.[3] In late May 2023, one cybercrime group exploited a critical software flaw within a file transfer platform (MOVEit), reportedly impacting over 60 million individuals and more than 2,600 organisations worldwide.[4] In the UK context, this incident enabled attackers to compromise a third-party HR company, likely exposing employees' personal data – including company IDs and national insurance numbers from organisations such as British Airways, Boots and the BBC – to organised cyber-criminals.[5] This may have been the largest ransomware incident of 2023, with a Russian-based threat actor linked to the CL0P ransomware operation claiming responsibility and demanding ransom payments in exchange for deleting the data.[6] It demonstrated ransomware threat actors' ability to continue to evolve their tactics and scale their operations to affect multiple victims in one operation.

The threat from ransomware shows no signs of abating, thanks to its profitable and innovative business model, poor cyber security practices in many organisations, and a permissive law enforcement environment in Russia.[7] No sector is off limits as threat actors continue to target public and private sector organisations,[8] schools,[9] hospitals and local government.[10]

[2] NCSC, 'NCSC Annual Review 2023', 14 November 2023, <https://www.ncsc.gov.uk/collection/annual-review-2023>, accessed 3 December 2023.

[3] Dan Milmo, 'Who is Behind the Latest Wave of UK Ransomware Attacks?', *The Guardian*, 14 September 2023.

[4] Zach Simas, 'Unpacking the MOVEit Breach: Statistics and Analysis', *Emsisoft*, 18 July 2023, <https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/>, accessed 3 December 2023.

[5] James Sillars, 'BA, BBC and Boots Hit by Cyber Security Breach with Contact and Bank Details Exposed', *Sky News*, 5 June 2023.

[6] Intel471, 'Insights from CLOP's MOVEit Extortion Attack', 22 June 2023, <https://intel471.com/blog/insights-from-clops-moveit-extortion-attack>, accessed 3 December 2023.

[7] Jamie MacColl et al., 'Cyber Insurance and the Ransomware Challenge', *RUSI Occasional Papers* (July 2023).

[8] BlackFog, 'The State of Ransomware 2023', November 2023, <https://www.blackfog.com/the-state-of-ransomware-in-2023/>, accessed 3 December 2023.

[9] MalwareBytes, 'The 2023 State of Ransomware in Education: 84% Increase in Attacks Over 6-Month Period', 5 June 2023, <https://www.malwarebytes.com/blog/threat-intelligence/2023/06/the-2023-state-of-ransomware-in-education-84-increase-in-known-attacks-over-6-month-period>, accessed 3 December 2023.

[10] Sam Sabin, 'Ransomware Gangs Zero in on Under-Resourced U.S. Cities and Towns', *Axios*, 16 May 2023, <https://www.axios.com/2023/05/16/ransomware-us-cities-towns-local-government-hackers>, accessed 3

However, the victims of these attacks rarely share their experiences. There are many reasons for this reticence, including legal reasons, reputational concerns, or even plain fear – ransomware groups use aggressive language and methods to increase the victims' propensity to pay a ransom. Consequently, the lack of reporting to law enforcement and cyber security agencies, and limited transparency on the part of victims (including in terms of communicating with the media) means that there is scant understanding of the range of harms experienced by victims during and after such incidents. This research paper addresses that gap, by speaking to victims or others associated with an incident.

By shining a light on the harms experienced by victims, this research provides a clearer picture of the harm caused by ransomware and therefore also the economic, societal and national security risks posed by ransomware groups to the UK and beyond. This is important for policymakers and industry, as a more holistic understanding of the harms stemming from ransomware will allow government to make more informed policy prioritisation choices so as to reduce the threat and help law enforcement, incident responders and organisations to better support victims.

At present, much of the coverage of ransomware focuses on the financial harm inflicted by ransomware incidents. This is understandable, as financial harm is a highly relevant impact that is both tangible and, at times, measurable. For example, media coverage often addresses the immediate financial impact of ransomware in the form of ransom payments and business continuity costs.[11] Similarly, several studies focus on the cost of data breaches or other cyber incidents, including ransomware attacks.[12] This paper does not seek to play down financial harm – indeed, ransomware causes wider financial harm than is usually recognised, but there are few studies that attempt to make a macroeconomic impact assessment of the harm from ransomware beyond the cost to a particular organisation.[13]

December 2023.

[11] Joe Tidy, 'How a Ransomware Attack Cost One Firm £45m', *BBC News*, 25 July 2019.

[12] Jason Blosil, 'Measuring the True Cost of a Ransomware Attack', *NetApp*, 24 October 2022, <https://www.netapp.com/blog/ransomware-cost/>, accessed 3 December 2023; IBM, 'Cost of a Data Breach Report 2023', 24 July 2023, <https://www.ibm.com/reports/data-breach>, accessed 3 December 2023.

[13] For an indicative sample of existing literature, see Aron Laszka, Sadegh Farhang and Jens Grossklags, 'On the Economics of Ransomware', in Stefan Rass et al. (eds), *Decision and Game Theory for Security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017, Proceedings* (Cham: Springer, 2017); Aaron Zimba and Mumbi Chishimba, 'On the Economic Impact of Crypto-Ransomware Attacks: The State of the Art on Enterprise Systems', *European Journal for Security Research* (Vol. 4, January 2019), pp. 3–31; Dietmar P F Möller, 'Ransomware Attacks and Scenarios: Cost Factors and Loss of Reputation', in Dietmar P F Möller, *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (Cham: Springer, 2023), pp. 273–303; Julio Hernandez-Castro, Edward Cartwright and Anna Stepanova, 'Economic Analysis of Ransomware', *arXiv*, March 2017, <https://arxiv.org/abs/1703.06660>, accessed 3 December 2023. Given the marked change in the nature of the ransomware threat from 2017 onwards, these endeavours should be considered part of an ongoing – cumulative – effort to assess the impact of ransomware.

However, there are a range of other harms from ransomware too, beyond the obvious financial impacts. These harms go beyond just affecting the direct victim of an incident – indirect victims can include other organisations, communities and individuals – and can be physical and psychological in nature. There is a real human impact to ransomware attacks that is yet to be fully grasped and measured.[14] Although some reporting has tried to focus on this aspect by exploring the impact of incidents on students and council tenants, or by exploring the psychological[15] and long-term harms caused by ransomware,[16] such reports remain few and far between.

Ransomware can ruin lives. This paper addresses the broader harms caused by ransomware, ranging from individual victims through to UK national security and prosperity. By engaging with victims and those associated with an incident, such as incident responders, insurers, lawyers, law enforcement officers and government officials, this research uncovers unique insights into a range of harms from ransomware. The findings should not only alert more policymakers to the scourge of ransomware, but also lead to a serious rethink about the resources required to combat ransomware in a meaningful way, both in the UK context and more widely.

Structure

This paper comprises three chapters. Chapter I sets outs out the tactics and techniques used by ransomware threat actors to cause harm. Chapter II details the harms that result from ransomware attacks, in an analysis based on interview data, workshops and public reporting; impacts from ransomware incidents are listed as first-, second- and/or third-order harms respectively. Chapter III sets out important implications for policymakers and practitioners to consider.

Methodology

This paper is part of a 12-month research project on ‘Ransomware Harms and the Victim Experience’. The project is funded by the UK’s NCSC and the Research Institute in Sociotechnical Cyber Security, and conducted by RUSI and the

[14] See Jamie MacColl, Pia Hüsch and Jason R C Nurse, ‘Beyond the Bottom Line: The Societal Impact of Ransomware’, *RUSI Commentary*, 14 November 2022.

[15] HelpNet Security, ‘The Long-Term Psychological Effects of Ransomware Attacks’, 25 October 2022, <https://www.helpnetsecurity.com/2022/10/25/psychological-effects-ransomware/>, accessed 3 December 2023; Joshua Crumbaugh, ‘The Psychological Warfare Behind Ransomware Attacks’, *Security Magazine*, 23 November 2022, <https://www.securitymagazine.com/articles/98654-the-psychological-warfare-behind-ransomware-attacks>, accessed 3 December 2023.

[16] Matt Burgess, ‘The Untold Story of a Crippling Ransomware Attack’, *Wired*, 31 January 2023, <https://www.wired.co.uk/article/ransomware-attack-recovery-hackney>, accessed 3 December 2023.

University of Kent. The paper's aim is to understand the wide range of harms caused by ransomware attacks to individuals, organisations and society at large.

The paper focuses on the question of what harms (for example, physical, economic, societal, psychological) ransomware incidents cause to organisations and individuals in the UK, and to the UK more broadly.

The data collection and analysis for this paper entailed a literature review, semi-structured interviews and workshops. One strength of the research approach is that participants were encouraged to speak freely about their own experience of ransomware attacks.

- **Literature review**: This consisted of 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 conducted by stakeholders in 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 interviews with victims of ransomware attacks and with subject matter experts from across the ransomware ecosystem, including individuals from the insurance industry, government and law enforcement, as well as incident responders. Interviews were conducted between November 2022 and March 2023, and were anonymised to allow individuals to speak openly about potentially sensitive issues. The research team then analysed the interview transcripts using NVivo data analysis software.[17] Throughout this paper, an anonymised coding system, based on Table 1, is used to refer to interview data in the footnotes.
- **Workshops**: In November 2022 and February 2023, the research team conducted two online workshops with key stakeholders from UK government, the insurance and cyber security industries, lawyers and law enforcement. Attendees included a mix of interviewees and new participants, using contacts established during the interview phase. The first workshop was used for data gathering and had 26 participants; the second was used to validate and reassess themes identified in the first workshop, the literature review and in interviews, and had 21 participants.

The paper focuses primarily on the harm caused in a UK context, but it also draws on experiences from other countries, such as the US. A small number of international participants were included in this research project.

[17] Lumivero, 'Nvivo', <https://lumivero.com/products/nvivo/>, accessed 11 January 2024.

Table 1: Interview Participants (Non-Victims/Victims)

Non-Victims	
Type of organisation	**Number of participants**
Digital Forensics and Incident Response (DFIR)	7
Ransomware Specialist	3
External Counsel	4
Insurance Claims	3
Crisis Communications	1
NCSC	2
Law Enforcement	2
Total (non-victims)	**22**
Victims	
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 (victims)	**20**

Source: Author generated.

Definitions

For the purpose of this paper, a 'victim' is any person or organisation that experiences harm as a result of a ransomware attack. This term can apply to individuals and organisations that are directly impacted, and to those that are indirectly affected and experience harm as a result. The term 'harm' refers to any negative impact the victim may experience, which could be of a financial, physical, psychological, reputational or other nature.[18] These underlying definitions are intentionally broad, allowing this paper to examine the full range of harms and victims that are impacted by ransomware attacks.

[18] Agrafiotis et al., 'A Taxonomy of Cyber-Harms', pp. 1–15.

Limitations

A number of factors limit the generalisability of the research's findings. First, the victim interviews should not be considered representative of a 'universal' victim experience. As identified in the research, there is variation in the harms experienced by different victims. Additionally, the interviews included more public sector than private sector victims, with a very limited number of small and medium-sized enterprises (SMEs) represented. Moreover, there may also be a self-reporting bias, given that the interview data is based on organisations that were happy to speak about the harm they experienced.

Second, the observations made in this paper are primarily about the UK. While many businesses – victims and those that are part of the cyber security ecosystem alike – provide services globally, the focus of this research rested on incidents and victims in the UK and their interactions with the UK cyber security ecosystem, including UK law enforcement and government.

I. Ransomware: Tactics and Targeting

Ransomware has historically been defined as a form of malware that disrupts a user's access to their computer system through encryption or locking. However, in recent years 'ransomware' has become a catch-all term for different types of cyber extortion – including data theft. As such, this paper follows the Ransomware Task Force's broader definition of ransomware as activity where threat actors compromise computer systems and demand a ransom for the restoration or non-exposure of encrypted and/or stolen data and systems.[19]

Creators of Harm: The Ransomware Ecosystem

Ransomware, after nearly a decade of growth and innovation, is a highly profitable criminal enterprise supported by a diverse and professionalised ecosystem.[20]

Although there is no fixed business model for ransomware threat actors, a recent joint report by the UK's NCSC and the National Crime Agency (NCA) outlined three broad business models that all cause harm to UK victims:[21]

- The 'buy-a-build' model, which usually involves smaller groups of less experienced cyber-criminals obtaining existing ransomware code to develop.
- The 'in-house' model, where the same organisation responsible for developing the ransomware also conduct the operations (although they may still rely on other parts of the cyber-criminal ecosystem for other services necessary to monetise ransomware).
- The 'ransomware-as-a-service' (RaaS) model, which involves collaboration between groups/individuals who develop and maintain the infrastructure

[19] Ransomware Task Force, 'Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force', Institute for Security and Technology, April 2021, p. 5, <https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf>, accessed 3 December 2023.

[20] John Sakellariadis, 'Behind the Rise of Ransomware', Atlantic Council, 2 August 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/>, accessed 3 December 2023; David S Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic', *European Law Enforcement Research Bulletin* (Issue 22, Summer 2022), pp. 45–60.

[21] NCSC, 'Ransomware, Extortion and the Cyber Crime Ecosystem', 11 September 2023, <https://www.ncsc.gov.uk/files/White-paper-Ransomware-extortion-and-the-cyber-crime-ecosystem.pdf>, accessed 20 November 2023.

and tools behind ransomware operations, and 'affiliates' who conduct operations for a percentage of profits.[22] This model has become dominant in the ransomware ecosystem and has enabled operators to scale and increase the volume of attacks, thereby increasing the amount of harm ransomware causes.

Ransomware operations are also supported by specialists in the criminal ecosystem, such as botnet operators, initial access brokers (who specialise in gaining access to victims' networks), negotiators and money launderers.

Methods of Harm: Extortion Tactics and Techniques

Ransomware criminals are profit-driven and have developed a range of tactics and techniques to extort payments from victims. These methods rest on causing harm (or the fear of potential harm) to victims to pressure them into ceding to threat actors' demands. Cyber-criminals use two primary extortion methods, although these are supported by a range of additional extortion tactics and techniques to increase their leverage.

Primary Extortion Methods

- **Encryption**: Encrypting data is the most common tactic used by ransomware threat actors. This approach involves gaining access to a victim's network, escalating privileges and accessing as many systems as possible before deploying malware that encrypts files and delivers the ransom note.[23] Although early 'pray-and-spray' ransomware campaigns only targeted individual endpoints, ransomware affiliates now aim to compromise domain administrator accounts so as to encrypt thousands of computers within a single organisation in one go. To maximise disruption and harm, threat actors will often spend time seeking out the critical systems and backups before encrypting them.[24] These attacks can be particularly harmful to organisations that rely on maintaining continuous operations.

[22] Mayra Fuentes et al., 'Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them', Trend Micro, 2021, p. 11, <https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf>, accessed 3 December 2023; Microsoft Threat Intelligence, 'Ransomware as a Service: Understanding the Cybercrime Gig Economy and How to Protect Yourself', 9 May 2022, <https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/>, accessed 3 December 2023; Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic'.

[23] James Sullivan and James Muir, 'Ransomware: A Perfect Storm', RUSI Emerging Insights, 2021, p. 7.

[24] *Ibid.*

- **Data theft**: Since late 2019, cyber-criminals have also adopted so-called 'double extortion' tactics, stealing victims' data as well as encrypting it, then threatening to leak it unless the ransom is paid.[25] Data theft can be a particularly useful tactic for targeting organisations with sensitive intellectual property, safeguarding data (such as schools) or medical data.[26] Stolen financial information, including accounting and insurance policies, can be used to help threat actors design negotiation strategies and set ransom demands. Recently, some ransomware operations have foregone encrypting victims' data altogether, and just stolen it.[27] This trend is in part driven by larger organisations' efforts to improve their resilience against ransomware by introducing offline backups and other measures, but also by the emergence in 2022 and 2023 of ransomware operations that exploit vulnerabilities in file transfer services, enabling criminals to steal data from dozens or even hundreds of victims at a time.[28]

Secondary Extortion Methods

After encrypting systems and/or stealing data, ransomware threat actors often use additional methods to raise the stakes for victims and disrupt their response and recovery.

- **Data leak sites**: Since adopting data theft tactics, ransomware operators have also launched 'name-and-shame' leak sites, on both the dark and clear webs, where they can name victims and leak data. This shames victims, but also serves as a warning to future victims who might consider refusing to pay. Threat actors can also draw additional attention to data leaks through social media or by contacting journalists.[29]

[25] Fuentes et al., 'Modern Ransomware's Double Extortion Tactics'.

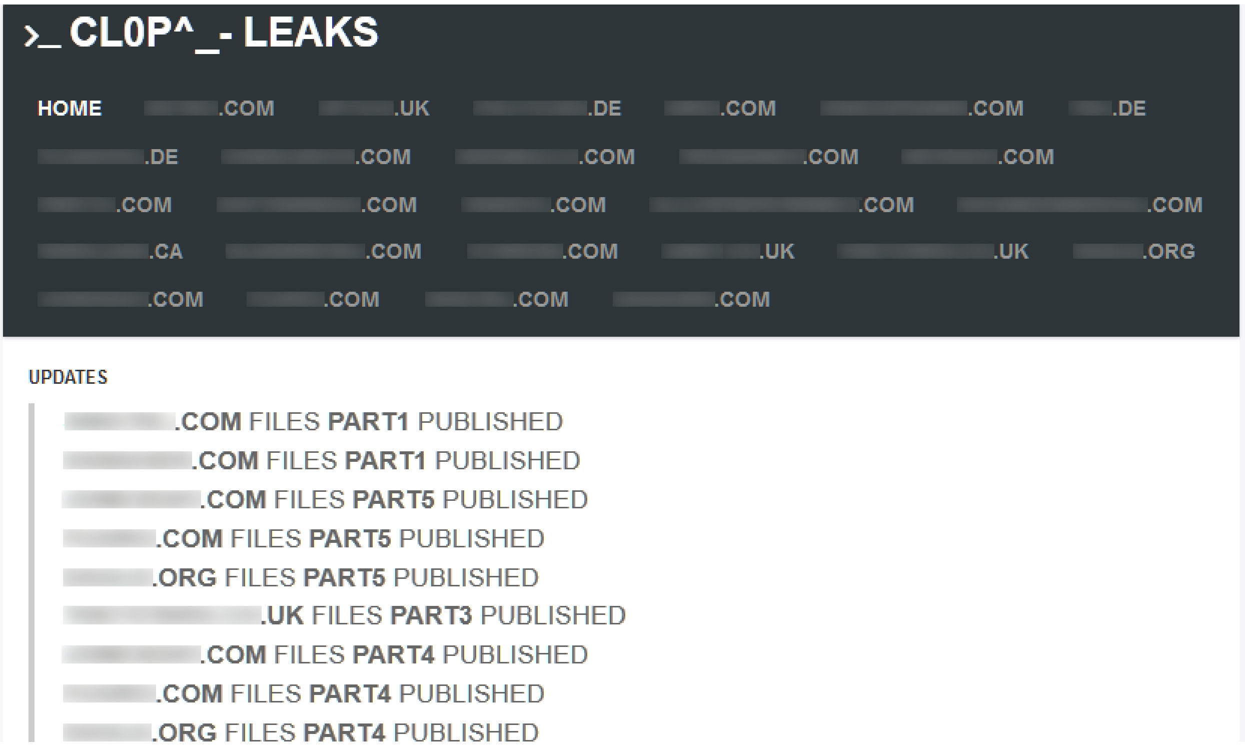
[26] *Ibid.*, p. 11; Office of Information Security, 'Data Exfiltration Trends in Healthcare', 9 March 2023, <https://www.hhs.gov/sites/default/files/data-exfiltration-in-healthcare-tlpclear.pdf>, accessed 3 December 2023.

[27] Jovi Umawing, 'Karakurt Extortion Group: Threat Profile', MalwareBytes, 14 June 2022, <https://www.malwarebytes.com/blog/news/2022/06/karakurt-extortion-group-threat-profile>, accessed 3 December 2023; Aleksander Milenkoski and Gijs Rijnders, 'Ransoms Without Ransomware, Data Corruption and Other New Tactics in Cyber Extortion', SentinelOne, 20 October 2022, <https://www.sentinelone.com/blog/ransoms-without-ransomware-data-corruption-and-other-new-tactics-in-cyber-extortion/>, accessed 3 December 2023; Unit 42, '2023 Ransomware and Extortion Report', p. 12, <https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/2023-unit42-ransomware-extortion-report.pdf>, accessed 3 December 2023.

[28] Unit 42, '2023 Ransomware and Extortion Report', p. 7.

[29] Tim Starks and Aaron Schaffer, 'For Ransomware Gangs, Journalists are Another Tool of the Trade', *Washington Post*, 10 August 2022.

Figure 1: The CL0P Data Leak Site Lists New Victims



>_ CL0P^_- LEAKS

HOME [redacted].COM [redacted].UK [redacted].DE [redacted].COM [redacted].COM [redacted].DE

[redacted].DE [redacted].COM [redacted].COM [redacted].COM [redacted].COM

[redacted].COM [redacted].COM [redacted].COM [redacted].COM [redacted].COM

[redacted].CA [redacted].COM [redacted].COM [redacted].UK [redacted].UK [redacted].ORG

[redacted].COM [redacted].COM [redacted].COM [redacted].COM

UPDATES

[redacted].COM FILES **PART1** PUBLISHED
[redacted].COM FILES **PART1** PUBLISHED
[redacted].COM FILES **PART5** PUBLISHED
[redacted].COM FILES **PART5** PUBLISHED
[redacted].ORG FILES **PART5** PUBLISHED
[redacted].UK FILES **PART3** PUBLISHED
[redacted].COM FILES **PART4** PUBLISHED
[redacted].COM FILES **PART4** PUBLISHED
[redacted].ORG FILES **PART4** PUBLISHED

Source: Cyberint, 'CL0P Ransomware: The Latest Updates', 23 October 2023, <https://cyberint.com/blog/techtalks/cl0p-ransomware/>, accessed 12 December 2023.

- **Harassment of employees and customers**: More aggressive ransomware threat actors will also directly contact an affected organisation's employees or customers.[30] This method can be untargeted – for instance, cold calling a company's phonelines in the hope that an employee will pick up; or more targeted – such as directly contacting executives or sending stolen personal data to relevant employees.[31] This can be particularly embarrassing – and involve reputational risk and commercial consequences – if cyber-criminals send stolen data to a victim's customers or users.[32] Some reporting suggests

[30] Connor Jones, 'BlackCat Ransomware Crims Threaten to Directly Extort Victim's Customers', *The Register*, 5 December 2023, <https://www.theregister.com/2023/12/05/alphvblackcat_shakes_up_tactics_again/>, accessed 8 December 2023.

[31] Catalin Cimpanu, 'Some Ransomware Gangs are Going After Top Execs to Pressure Companies into Paying', *ZDNet*, 9 January 2021, <https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/>, accessed 3 December 2023.

[32] Pieter Arntz, 'Ransomware Gangs are Recruiting Breached Individuals to Persuade Companies to Pay Up', MalwareBytes, 27 January 2022, <https://www.malwarebytes.com/blog/news/2022/01/ransomware-gangs-are-recruiting-breached-individuals-to-persuade-companies-to-pay-up>, accessed 3 December 2023; Lawrence Abrams, 'Ransomware Gang Urges Victims' Customers to Demand a Ransom Payment', *Bleeping Computer*, 26 March 2021, <https://www.bleepingcomputer.com/news/security/ransomware-gang-urges-victims-customers-to-demand-a-ransom-payment/>, accessed 3 December 2023.

that ransomware threat actors are adopting more extreme forms of harassment as victims' willingness to pay ransoms decreases.[33]

- **DDoS attacks**: Ransomware threat actors have also been known to use distributed denial-of-service (DDoS) attacks to increase disruption to victims' digital infrastructure.[34] However, industry reporting indicates that this is not a widely used tactic: for instance, a report by the cyber security vendor Unit 42 (part of Palo Alto Networks), suggested that only 2% of the ransomware incidents they responded to in 2022 involved a DDoS attack as part of the extortion attempt.[35]

Who Experiences Harm: Ransomware Targeting and Victimisation

Ransomware threat actors are largely agnostic about who they choose to target, which means that almost any organisation is a potential ransomware victim.[36] However, there are several considerations that, to varying degrees, appear to influence ransomware targeting and victimisation.

- **Opportunism**: Ransomware affiliates either gain access to organisations themselves or use specialist access brokers. In either case, organisations are typically compromised through opportunistic tactics and techniques that are designed to gain access to a wide range of victims through scanning for internet-facing vulnerabilities or poorly secured remote desktop protocols, or via phishing campaigns.[37] This makes organisations and sectors that underinvest in or mismanage IT infrastructure and cyber security particularly vulnerable to ransomware.
- **Nature of business/organisation**: Some ransomware threat actors appear to prioritise organisations that are incentivised to quickly resolve incidents.[38] Criminals often seek targets for whom it is critical that their operations

[33] Frank Bajak, Heather Hollingsworth and Larry Fenn, 'Ransomware Criminals are Dumping Kids' Private Files Online After School Hacks', *AP News*, 5 July 2023, <https://apnews.com/article/schools-ransomware-data-breach-40ebeda010158f04a1ef14607bfed9b0>, accessed 3 December 2023; Unit 42, '2023 Ransomware and Extortion Report', p. 6.

[34] Canadian Centre for Cyber Security, 'Baseline Cyber Threat Assessment: Cybercrime', August 2023, <https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime>, accessed 3 December 2023; New Jersey Cybersecurity & Communications Integration Cell, 'The Evolution of Ransomware: A 5-Year Perspective', 26 July 2023, <https://www.cyber.nj.gov/informational-report/the-evolution-of-ransomware-a-5-year-perspective>, accessed 3 December 2023.

[35] Unit 42, '2023 Ransomware and Extortion Report', p. 6.

[36] NCSC, 'Ransomware, Extortion and the Cyber Crime Ecosystem'.

[37] MacColl et al., 'Cyber Insurance and the Ransomware Challenge', pp. 36–37.

[38] 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 29 April 2022.

provide certain products or services in a timely manner. Alternatively, being attuned to the potential regulatory and reputational risks that the exposure of customer or client data can entail, they might prioritise organisations that hold sensitive information. This means that victims may be targeted by virtue of the vulnerabilities linked to their industry sector. While some ransomware actors adopt a risk-averse avoidance of critical national infrastructure (CNI) sectors (although this is unlikely to be an absolute commitment to avoid disrupting such sectors), others prioritise their targeting based on the assumption of an increased likelihood of payment.[39] Some ransomware groups were relentless in their targeting of healthcare organisations during the Covid-19 pandemic,[40] while one more recent ransomware operation, Vice Society, has focused on targeting and stealing sensitive data from education providers in the US and the UK.[41]

- **Size of organisation**: Some threat actors deliberately target larger organisations. So-called 'big game hunting' ransomware operations aim to generate sizeable pay-outs from large corporations.[42] However, size does not matter for most ransomware threat actors, and reporting from Coveware, a specialist ransomware response firm, consistently highlights that the median ransomware victim is a medium-sized organisation.[43]

Taken together, these factors emphasise that a wide range of organisations (and by extension, their employees and customers, or users of their products and services) can be harmed by ransomware. The rest of this paper examines the impact of ransomware on organisations, individuals and society.

[39] For targeting of schools and healthcare, see, for example, Ransomware Task Force, 'Combating Ransomware', pp. 8–10.

[40] Brian Krebs, 'Conti's Ransomware Toll on the Healthcare Industry', *Krebs On Security*, 18 April 2022, <https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/>, accessed 3 December 2023.

[41] J R Gumarin, 'Vice Society: Profiling a Persistent Threat to the Education Sector', Unit 42, 6 December 2022, <https://unit42.paloaltonetworks.com/vice-society-targets-education-sector/>, accessed 3 December 2023; Jonathan Holmes, 'Schools Hit by Cyber Attack and Documents Leaked', *BBC News*, 6 January 2023.

[42] CrowdStrike, 'Cyber Big Game Hunting', 21 March 2022, <https://www.crowdstrike.com/cybersecurity-101/cyber-big-game-hunting/>, accessed 3 December 2023.

[43] Coveware, 'Ransom Monetization Rates Fall to Record Low Despite Jump in Average Ransom Payment', 21 July 2023, <https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments>, accessed 3 December 2023.

II. Ransomware Harms

This chapter identifies the range of harms that organisations, individuals and countries such as the UK experience as a result of a ransomware incident. The findings build on existing research that analyses or categorises ransomware or cyber breach harms. Existing research has, for instance: drawn a distinction between 'direct' and 'indirect' harms to a victim (particularly financial);[44] explored cumulative impacts, such as reduced employee productivity;[45] emphasised the potential societal impacts arising from protracted CNI downtime;[46] articulated the risk of tangible loss of reputation;[47] considered psychological harms experienced by impacted individuals;[48] and reflected on the broader range of impacts that may be experienced by clients, including hospital patients and school students.[49]

[44] Department for Science, Innovation & Technology (DSIT), 'Cyber Security Breaches Survey 2023', 19 April 2023, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023>, accessed 3 December 2023; Department for Digital, Culture, Media & Sport (DCMS), 'Cyber Security Breaches Survey 2022', 11 July 2022, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>, accessed 3 December 2023; Harry Heyburn et al., 'Analysis of the Full Costs of Cyber Security Breaches', IPSOS Mori Public Affairs 2020, <https://assets.publishing.service.gov.uk/media/5f117e51d3bf7f5bae197869/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf>, accessed 3 December 2023; Deloitte, 'Beneath the Surface of a Cyberattack: A Deeper Look at Business Impacts', 2016, <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-beneath-the-surface-of-a-cyber-attack.pdf>, accessed 3 December 2023; Samir Jarjoui, Robert Murimi and Renita Murimi, 'Hold My Beer: A Case Study of How Ransomware Affected an Australian Beverage Company', in *Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, 2021*, <https://ieeexplore.ieee.org/document/9478239>, accessed 3 December 2023; Jay Kesan and Linfeng Zhang, 'Analysis of Cyber Incident Categories Based on Losses', *ACM Transactions on Management Information Systems*, forthcoming, University of Illinois College of Law Legal Studies Research Paper No. 20-8, posted 22 November 2019, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3489436>, accessed 3 December 2023.

[45] Mark Button et al., 'From Feeling Like Rape to a Minor Inconvenience: Victims' Accounts of the Impact of Computer Misuse Crime in the United Kingdom', *Telematics and Informatics* (Vol. 64, November 2021).

[46] Ransomware Taskforce, 'Combating Ransomware'.

[47] DSIT, 'Cyber Security Breaches Survey 2023'; DCMS, 'Cyber Security Breaches Survey 2022'; Anthony Freed, 'How Do Ransomware Attacks Impact Victim Organisations' Stock?', Cybereason, 2022, <https://www.cybereason.com/blog/how-do-ransomware-attacks-impact-victim-organizations-stock>, accessed 3 December 2023.

[48] Button et al., 'From Feeling Like Rape to a Minor Inconvenience'; Ryan Shandler and Miguel Gomez, 'The Hidden Threat of Cyber-Attacks – Undermining Public Confidence in Government', *Journal of Information Technology and Politics* (Vol. 20, Issue 4, August 2022); Leah Zhang-Kennedy et al., 'The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution', *Proceedings of the 27th USENIX Security Symposium, August 15–18 2018, Baltimore, MD*, <https://www.usenix.org/conference/usenixsecurity18/presentation/zhang-kennedy>, accessed 3 December 2023; Jane Zhao et al., 'Impact of Trauma Hospital Ransomware Attack on Surgical Residency Training', *Journal of Surgical Research* (Vol. 232, December 2018); Maria Bada and Jason Nurse, 'The Social and Psychological Impact of Cyberattacks', in Vladlena Benson and John McAlaney (eds), *Emerging Cyber Threats and Cognitive Vulnerabilities* (Cambridge, MA: Academic Press, 2020), pp. 73–92.

[49] Kitty Kioskli, Theo Fotis and Haralambos Moutatidis, 'The Landscape of Cybersecurity Vulnerabilities and Challenges in Healthcare: Security Standards and Paradigm Shift Recommendations', *ARES '21:*

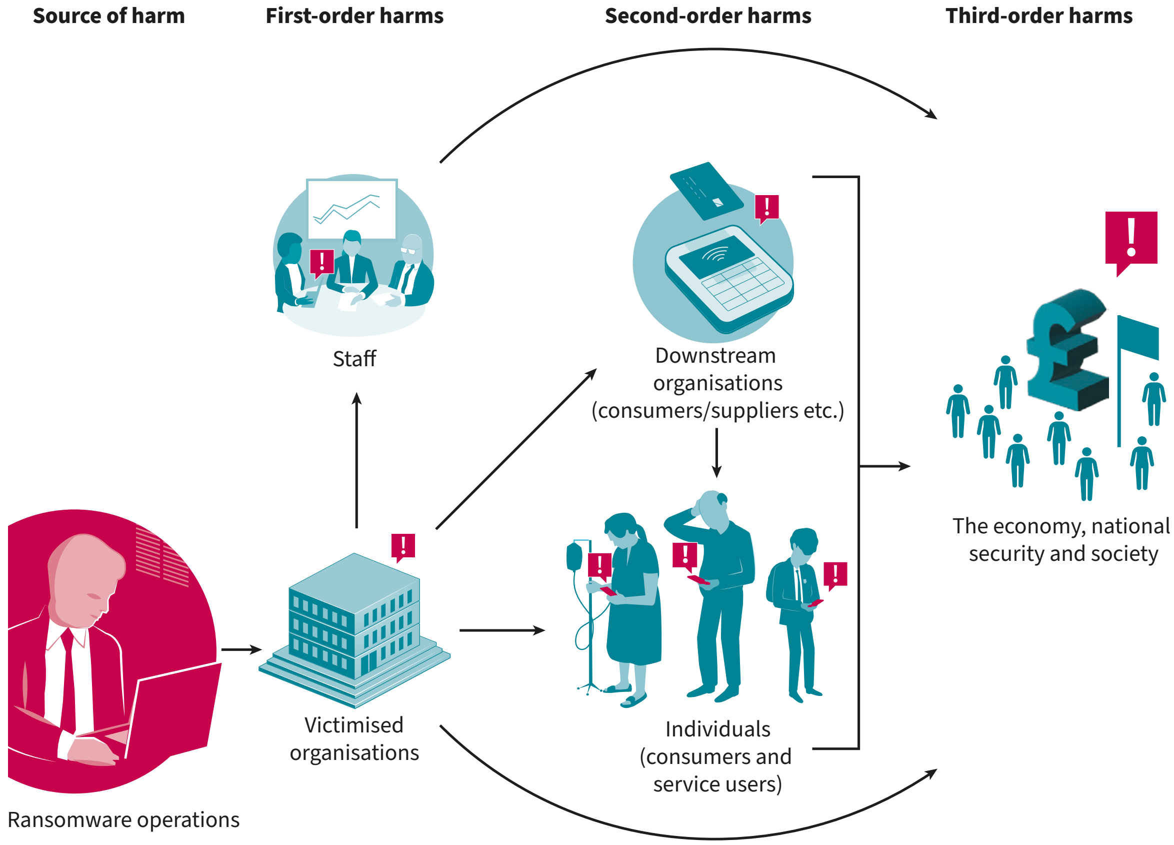
To improve understanding of the different types of harm caused by ransomware across society and to help understand the scale of the policy challenge, this paper uses a framework with three categories:[50]

- **First-order harms:** Harms to any organisation (and its staff) directly targeted by a ransomware operation.
- **Second-order harms:** Harms to any organisation or individuals that are indirectly affected by a ransomware incident (e.g. organisations that are customers or clients of a victim, or individuals that are customers of a victim or use a service that is disrupted).
- **Third-order harms:** The cumulative effect of incidents on wider society, the economy and national security.

Proceedings of the 16th International Conference on Availability, Reliability and Security, 2021, <https://dl.acm.org/doi/abs/10.1145/3465481.3470033>, accessed 3 December 2023; Nikki Spence et al., 'Ransomware in Healthcare Facilities: A Harbinger of the Future?', *Perspectives in Health Information Management* (Summer 2018); Thomas Slayton, 'Ransomware: The Virus Attacking the Healthcare Industry', *Journal of Legal Medicine* (Vol. 38, Apr–Jun 2018); Noor Thamer and Raaid Alubady, 'A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research', paper presented to the 1st Babylon International Conference on Information Technology and Science, Babil, Iraq, 28–29 April 2021, <https://ieeexplore.ieee.org/document/9509877>, accessed 3 December 2023; Zhang-Kennedy et al., 'The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution'; Usman Butt, Yusuf Dauda and Baba Shaheer, 'Ransomware Attack on the Educational Sector', in Hamid Jahankhani et al. (eds), *AI, Blockchain and Self-Sovereign Identity in Higher Education* (Cham: Springer, 2023), pp. 279–313.

[50] For indicative existing research that draws on orders of cyber harms, see Erwin Orye and Olaf M Maennel, 'Recommendations for Enhancing the Results of Cyber Effects', paper presented to the 11th International Conference on Cyber Conflict, Tallinn, Estonia, 28–31 May 2019, <https://ccdcoe.org/uploads/2019/06/Art_06_Recommendations-for-Enchasing-the-Results-of-Cyber-Effects.pdf>, accessed 8 December 2023; Martin Pergler and Eric Lamarre, 'Upgrading Your Risk Assessment for Uncertain Times', McKinsey, January 2009, <https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/9_upgrading_your_risk_assessment_for_uncertain_times.ashx>, accessed 3 December 2023.

Figure 2: The Three Different Categories of Ransomware Harms, and Who/What They Affect


Source of harm
First-order harms
Second-order harms
Third-order harms
Staff
Downstream organisations (consumers/suppliers etc.)
The economy, national security and society
Ransomware operations
Victimised organisations
Individuals (consumers and service users)

Source: Author generated.

Figure 2 illustrates how ransomware attacks can cascade through the supply chain, economy and society, distinguishing between harms that are experienced by organisations, individuals and countries. Some harms impact the organisations directly targeted by ransomware, others impact organisations and individuals indirectly affected by ransomware.

This analysis draws on a 2018 taxonomy of cyber harms, which identifies five broad types of harm: physical or digital; financial or economic; reputational; psychological; and social or societal.[51] These five themes are applied to the three categories in the framework to illustrate the range of harms that organisations, individuals and countries can suffer. Each order of harm is contextualised using an author-generated figure, the content of which was derived from interviews and workshop data.

Crucially, this framework is not intended to be definitive. It builds on previous research and should be added to in the future. We urge policymakers, researchers and practitioners to continue to identify new types of harms based on further

[51] Agrafiotis et al., 'A Taxonomy of Cyber-Harms', pp. 1–15.

case studies and personal experiences, particularly with regard to sectors not represented in our evidence base. New types of harm will no doubt emerge as ransomware operators find new ways to harm and extort their victims.

First-Order Harms

The first category involves harms to the organisations and staff directly targeted by ransomware. Interview and workshop data highlighted areas of convergence and divergence between 'organisation' and 'staff' harm, to the extent that it is necessary to distinguish overtly between the two. The distinction between an organisation and individuals (and the harm they experience) is less apparent for small business owners or sole traders. They typically do not distinguish between the organisation and themselves, and might not have any other employees.

Figure 3: Categorisation of First-Order Harms to Organisations and Their Staff

Organisation				Staff				
Physical/digital harm	Financial harm: additional costs	Financial harm: financial loss	Reputational harm (internal and external)	Psychological harm	Physical harm	Financial harm	Reputational harm	Social harms
Systems/data encrypted	Ransom payment	Loss due to business interruption	Loss of client trust	Stress	Exhaustion	Job losses	Negative perception of professional skills	Strained relations with co-workers
Systems/data corrupted or destroyed	Cost of hiring response services (DFIR, lawyers, PR, etc.)	Loss of expected income	Loss of trust from regulators	Burnout	Sleep deprivation	No payment of salary	Risk of losing job as a result	Strained family life
Backups encrypted	Compensation for extra staff time	Loss/destruction of products	Loss of trust from employees/future employees	Confusion	Dehydration	Costs for therapy	Loss of trust from clients and peers	
Backups corrupted or destroyed	Hiring additional staff	Loss of customers/clients	Negative media reporting	Anger	Weight loss	Costs due to cancelled plans (e.g. holidays)		
IT infrastructure switched offline or isolated	Replacing staff (e.g. due to higher turnover or burnout)	Loss of staff time (e.g. due to additional tasks or burnout)		Panic	Burnout			
Prolonged reduced performance of IT infrastructure	Cost of counselling for staff	Reduced financial reserves		Worry/fear (e.g. of losing job)	Serious illness (e.g. heart conditions or stroke)			
Data exfiltrated	Cost of additional services (from providing food to credit monitoring)	Loss of intellectual property		Guilt	Hospitalisation			
Data leaked	Cost of replacing technology			Shame/self-blame				
Loss of access to customer systems	Increased cyber security costs			Doubt and resignation				
Physical systems (e.g. operational technology) disrupted	Increased cyber insurance premiums			Isolation				
CCTV, fire and/or estate control systems disrupted	Regulatory fines			Impact on personal relations (e.g. family life)				
	Litigation costs			Serious mental health conditions (e.g. suicidal thoughts)				
	Opportunity costs							

Source: Author generated.

First-Order Harms to Organisations

At the organisational level, this research has identified three main types of harm caused by ransomware: physical/digital harm to systems and data; financial harm; and reputational harm. While general reporting on ransomware harms often focuses on the immediate financial harm, for example, when media reporting stresses the size of a ransomware payment,[52] the research data indicates that the range of harm experienced by the victim organisation is much broader. The following section identifies themes that emerged from the research data.

Digital and Physical Harm

This category of harm describes negative impacts on an organisation's digital and physical systems, and on its data. Broadly, such harm results from the effects of ransomware threat actors' efforts to encrypt systems or steal data, and sometimes, in turn, from defenders' efforts to contain an incident.

Ransomware attacks involving encryption can have a profound negative impact on an organisation's IT infrastructure. Several of the victims interviewed revealed that their servers had been encrypted by the ransomware in their entirety,[53] with one victim in the education sector losing access to more than 10,000 computers as a result.[54] The impact becomes even more significant if ransomware operators are also able to encrypt or delete any backups. Interviewees also highlighted how common it is for cyber-criminals to deploy ransomware at the end of the week or during public holidays, when organisations are slower to react and defend themselves.[55]

The extent of disruption to IT infrastructure from ransomware varies from incident to incident. One government agency described how, in the aftermath of the ransomware deployment, 'we had lost access to all of our systems and … all of our data. We were right back to being a non-digital non-IT organisation'.[56] Indeed, a number of interviewees highlighted how, in the absence of key digital

[52] Sead Fadilpašić, 'Ransomware Payments Set to Hit a New High in 2023 – Here's How to Stay Safe', *Tech Radar Pro*, 13 July 2023, <https://www.techradar.com/pro/ransomware-payments-set-to-hit-a-new-high-in-2023-heres-how-to-stay-safe>, accessed 3 December 2023.

[53] Author interview with Local Government 1, 15 December 2022; author interview with Technology 3, 24 March 2023; author interview with Financial Services 1, 9 December 2022; author interview with Education 3, 10 January 2023; author interview with Government Agency 1, 3 March 2023; author interview with Professional Services 1, 17 March 2023.

[54] Author interview with Education 3, 10 January 2023.

[55] Author interview with Education 1, 8 December 2022; author interview with Education 2, 16 December 2022; author interview with Education 3, 10 January 2023; author interview with Charity 1, 12 January 2023; author interview with Government Agency 1, 3 March 2023; author interview with Engineering 1, 10 March 2023.

[56] Author interview with Government Agency 1, 3 March 2023.

services, ransomware often forces organisations to return to operating by 'pen and paper'.[57]

In other cases, ransomware can be isolated to a single server or IT function, either because it fails to deploy as planned or because security controls or resilience measures are (at least partially) effective.[58] However, even in these cases, the effort to contain ransomware can still have significant impacts on the delivery of business operations. Several interviewees highlighted how they had to disconnect or isolate their IT infrastructure from the internet for several days – or even weeks – while they assessed the extent of the attack and removed the threat actor's access to their networks.[59] The impact from drastic incident response measures can be as harmful to operations as the initial infection.

A ransomware attack and the subsequent recovery efforts can also result in prolonged reduced performance of IT infrastructure. Although some victims are able to recover within weeks or months, interviewees reported that recovery efforts can sometimes stretch into years. One interviewee from the professional services sector emphasised that their company still had trouble with impacted financial systems several years after the incident.[60] Hackney Council, which was targeted by cyber-criminals using Pysa ransomware in October 2022, took more than two years to recover fully from the incident.[61] And if backups are encrypted or destroyed, organisations may lose access to data permanently. One interviewee from the education sector, for instance, highlighted how teachers permanently lost teaching material following an attack against their academy trust, with some losing 20 years' worth of resources.[62]

Ransomware can also harm physical systems and processes. Although most ransomware operations lack the capability to directly compromise industrial control systems (ICS) and operational technology (OT), the disruption of IT infrastructure can cause cascading operational impacts.[63] Indeed, the increasing convergence of IT and OT leaves physical infrastructure more vulnerable to

[57] Author interview with Education 2, 16 December 2022; author interview with Government Agency 1, 3 March 2023; author interview with Financial Services 1, 9 December 2022; author interview with Education 3, 10 January 2023; author interview with Local Government 1, 15 December 2022; author interview with Local Government 2, 1 March 2023.

[58] Author interview with Technology 1, 20 March 2023; author interview with Charity 1, 12 January 2023; author interview with Engineering 1, 10 March 2023.

[59] Author interview with Education 1, 8 December 2022; author interview with Outsourcing 1, 15 December 2022; author interview with Education 2, 16 December 2022; author interview with Education 3, 10 January 2023; author interview with Engineering 1, 10 March 2023; author interview with Technology 1, 20 March 2023.

[60] Author interview with Professional Services 1, 17 March 2023.

[61] Burgess, 'The Untold Story of a Crippling Ransomware Attack'.

[62] Author interview with Education 4, 10 March 2023.

[63] Danny Palmer, 'Ransomware Gangs Now have Industrial Targets in Their Sights. That Raises the Stakes for Everyone', *ZDNet*, 2 February 2021, <https://www.zdnet.com/article/ransomware-gangs-now-have-industrial-targets-in-their-sights-that-raises-the-stakes-for-everyone/>, accessed 3 December 2023.

ransomware. One notable example is the 2019 ransomware attack on Norsk Hydro, a Norwegian aluminium and hydroelectric producer, which caused several plants to shut down at great cost.[64] A small number of the victims interviewed for this research paper used ICS as a core part of their business or operations, but most did not. Nonetheless, several interviewees highlighted examples where disruption to their IT digital infrastructure had knock-on effects on their operations. These included schools that lost access to CCTV, fire control systems, and doors and gates,[65] and a victim in the education sector that lost control over fridges and freezers containing sensitive research.[66]

Financial Harm

Victims of ransomware attacks experience a wide range of financial harm. Some forms of financial harm – such as the cost of a ransom payment – can be measured relatively easily, with studies finding that both ransom demands and incident response costs are steadily increasing.[67] Other aspects of financial harm are harder to quantify, such as the cost of missed opportunities and reduced productivity.[68] This means that there is limited understanding of the long-term financial harm caused by ransomware attacks.

Overall, interview data confirmed that, in line with wider public reporting,[69] primary attention rests on immediate financial harm, for example in the form of the additional costs encountered from a ransom payment, or losses arising from business interruption. One notable finding is that interviewees from victim organisations frequently reported that senior leadership would make assessments of the cost of the given ransomware incident, although it was challenging to disaggregate the overall costs of the ransomware incident from other fiscal shocks that occurred in the same timeframe as the incident, such as the Covid-19 pandemic.[70] These assessments would typically have a tightly restricted readership.[71] The interviews also confirmed that many organisations generally

[64] Microsoft, 'Hackers Hit Norsk Hydro with Ransomware. The Company Responded With Transparency', *Microsoft News*, 16 December 2019, <https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/>, accessed 7 July 2023.

[65] Author interview with Education 2, 16 December 2022; author interview with Education 4, 10 March 2023.

[66] Author interview with Education 3, 10 January 2023.

[67] IBM, 'Cost of a Data Breach Report 2023'; Allianz, 'Allianz Risk Barometer 2023', January 2023, <https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2023-cyber-incidents.html>, accessed 3 December 2023; Gareth Mott et al., 'Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era', *Computers & Security* (Vol. 128, May 2023).

[68] Zhang-Kennedy et al., 'The Aftermath of a Crypto-Ransomware Attack at a Large Academic Institution'.

[69] For example, Dole, the fresh vegetables business, reported that a ransomware attack cost the company $10.5 million in direct costs. See David Jones, 'Dole Incurs $10.5M in Direct Costs from February Ransomware Attack', *Cybersecurity Dive*, 18 May 2023, <https://www.cybersecuritydive.com/news/dole-10m-costs-ransomware/650711/>, accessed 3 December 2023.

[70] Author interview with Financial Services 1, 9 December 2022.

[71] *Ibid*.

have limited understanding of the overall financial impact a ransomware attack has on the organisation, particularly with respect to financial harm that is not covered by an insurance policy, or which plays out over the long term. Therefore, the data represented here is subject to the same limitations: assessments of financial impact are unlikely to be definitive, and there is a need for further research in this area. Given the scale and depth of ransomware as an impactful form of contemporary cybercrime affecting almost all organisational sectors, it is important to further collective understanding of the scale of this harm to individual organisations and the wider economy.

Additional Costs

Immediate financial harm spans the cost of paying the ransom itself and hiring external parties to help with the response to the incident – for example, incident response teams and lawyers, but also PR professionals. Often, the costs of hiring such third parties far exceeds the demand for the ransom payment.[72] Some providers, such as lawyers, are costly, especially when incidents are complex.[73] The high additional costs of hiring help from third parties are financially challenging where they are not covered by insurance, especially for small companies or for public service providers with limited financial reserves.[74]

Additional costs may also be incurred from paying existing staff overtime, or from hiring new (or temporary) staff. A victim from the education sector, for example, paid employees extra during the initial response phase, but also hired a cryptocurrency broker to facilitate access to cryptocurrency.[75]

But additional costs can also occur in less expected ways: one victim in the education sector was no longer able to charge students for school meals, and as a result had to cover the cost of food in the interim.[76] Some companies also offered to pay for counselling services for their staff, but these costs are typically not covered by insurance.[77] Some organisations also paid for credit monitoring for their employees.[78]

[72] Mott et al., 'Between a Rock and a Hard(ening) Place'.

[73] Josephine Wolff, *You'll See This Message When It is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches* (Cambridge, MA: MIT Press, 2018).

[74] Martin Wilson et al., 'It Won't Happen to Me: Surveying SME Attitudes to Cyber-Security', *Journal of Computer Information Systems* (Vol. 63, Issue 2, 2022).

[75] Author interview with Education 1, 8 December 2022.

[76] Author interview with Education 2, 16 December 2022.

[77] Author interview with Engineering 1, 10 March 2023.

[78] Author interview with Professional Services 1, 17 March 2023.

Many victims also face additional costs due to increased insurance premiums. While interviewees were often able to renew their cyber insurance policy after a ransomware attack, they had to do so at a higher cost.[79]

In the immediate reaction to a ransomware attack, additional costs may arise when replacing technology, as a ransomware attack often infiltrates many devices, or impairs communications for the victim. The victim may have to acquire additional devices, as was the case for one interviewee, who described how their company replaced all its employees' phones after a ransomware attack.[80] When phone systems in a local government entity failed due to a ransomware attack, extra telephones and mobile phones had to be acquired to enable staff to communicate with local citizens.[81] Another victim purchased large numbers of Chromebook devices to access their Microsoft 365 environment so as to enable communication between employees and with clients.[82]

Further significant, long-term costs are accrued when improving cyber security measures and updating IT networks.[83] While these measures are not always strictly required in response to a ransomware attack, such incidents often create the impetus for increased cyber security measures and spending. The costly decision to 'build back better' is often deemed necessary or even overdue, but not covered by insurance. As a victim in the education sector said, 'It's all a lot of money, but money we should have spent a year earlier'.[84]

Other long-term costs stem from regulatory fines, although in the UK it is not clear how many fines have been issued to victims of ransomware by the Information Commissioner's Office.[85] Moreover, decisions on these fines are often only delivered months or even years after an attack,[86] in the meantime weighing on a victim's mental health and limiting their ability to move on after the incident. Similarly, litigation costs may also only arise months or years after the ransomware attack has occurred.[87] Again, victims often require legal support during these processes, dragging out the additional costs incurred for hiring third parties such as data protection lawyers.

[79] Author interview with Charity 1, 12 January 2023; author interview with Consultancy 2, 17 March 2023.

[80] Author interview with Manufacturing 1, 27 January 2023.

[81] Author interview with Local Government 2, 1 March 2023.

[82] Author interview with Engineering 1, 10 March 2023.

[83] For example, author interview with Education 4, 10 March 2023.

[84] Author interview with Education 1, 8 December 2022.

[85] 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 3 December 2023.

[86] NCSC, 'Solicitors Urged to Help Stem the Rising Tide of Ransomware Payments', 8 July 2022, <https://www.ncsc.gov.uk/news/solicitors-urged-to-help-stem-the-rising-tide-of-ransomware-payments>, accessed 3 December 2023.

[87] Burgess, 'The Untold Story of a Crippling Ransomware Attack'.

While some additional costs come in the form of clearly defined bills, others are harder to directly trace back to the ransomware attack. One example of this is the additional cost of employee turnover. While some individuals might lose (or leave) their jobs directly as a result of an attack and need to be replaced, employees' decisions to leave often have more than one cause. A ransomware attack may be a contributing factor or the tipping point in a decision process, for example due to the stress or anxiety the attack evoked. Other influencing factors – such as the Covid-19 pandemic or an organisation's existing internal dynamics – make it hard to isolate a ransomware attack as the sole factor causing employee turnover.[88] Nevertheless, exit interviews in the education sector revealed that some teachers leaving the profession cited the ransomware attack as a tipping point, due to some of their data being lost to the attack – something they felt their employer should have protected them from.[89] Another victim described how the ransomware attack led to lower morale among employees, which in turn had 'a knock-on effect as people started to leave. It makes those people that are on the fence of … leaving make that decision'.[90] Low morale and other such intangible influences take a long time to overcome, the interviewee noted.[91]

For other interviewees, ransomware incidents were clearly the reason why people left their jobs, for example due to stress levels experienced during the ransomware response or because the person's account had been used by the hacker (and, although this was not their fault, the repeated mentioning of their name throughout the response led to them leaving the organisation in question).[92]

Higher costs due to employee turnover may also arise because experienced IT staff receive more attractive employment offers from elsewhere. An interviewee in the engineering sector explained that 'trying to hold on to people who are battle-tested in that kind of space is extremely difficult because everybody wants them'.[93]

In addition, higher costs may occur where staff needs to be – temporarily – replaced due to burnout or other psychological harm. For example, one interviewee described how staff were unable to return to work for months after the ransomware response due to the high stress levels experienced.[94]

Finally, victims often experience a more intangible type of cost: opportunity costs, wherein budgeting is disrupted by the need to redirect resources away

[88] Author interview with Local Government 1, 15 December 2022.
[89] Author interview with Education 4, 10 March 2023.
[90] Author interview with Professional Services 1, 17 March 2023.
[91] *Ibid*.
[92] Author interview with DFIR 1, 5 December 2022.
[93] Author interview with Engineering 1, 10 March 2023.
[94] Author interview with Financial Services 1, 9 December 2022.

from other objectives. A recent survey of 100 directors of UK firms impacted by ransomware identified that their organisations cut operating costs by an average of 17% following their ransomware incident.[95]

The impact of opportunity costs is likely to affect all victims operating with constrained finances, but may be particularly noticeable for victims in the public sector, such as councils, schools or hospitals, which are already running on tight budgets and have little ability to build back reserves. One interviewee in the public sector described how further cuts in funding put them in a worse position now than they were when the attack occurred, and that, in order to build back reserves, the organisation had to be particularly frugal in its spending and to increase revenue sources.[96] In other ways, opportunity costs stem from reductions in productivity or from diverting staff from other pressing priorities to work on recovering from an incident.

Ransomware victims thus encounter additional costs in many ways, some of which are better anticipated than others. These additional costs often exceed the ransom demand by a significant degree. Moreover, many additional costs only occur in the long term, such as litigation costs or the cost of building back IT networks. Long-term costs can also arise as a consequence of other harms, for example when new employees need to be hired after former employees leave their positions or need to be replaced due to burnout. Some of these costs are covered by insurance providers, but where this is not the case, ransomware victims often have limited insights into the long-term additional costs they face.

Financial Losses

As well as the additional costs a victim organisation may face due to a ransomware attack, it may also experience a number of financial losses; indeed, small businesses may face the threat of going out of business.[97] Even where the financial losses do not present an existential threat, they can nevertheless be significant. The following paragraphs provide some examples of the kind of financial losses that can occur.

Business interruption accounts for the majority of financial losses after a ransomware attack[98] – for example, when a company is unable to produce

[95] Phil Muncaster, 'Ransomware Surge is Driving UK Inflation, Says Veeam', *InfoSecurity Magazine*, 8 December 2023, <https://www.infosecurity-magazine.com/news/ransomware-surge-driving-uk/>, accessed 8 December 2023.

[96] Author interview with Local Government 2, 1 March 2023.

[97] Author interview with DFIR 1, 5 December 2022.

[98] Cynthia Brumfield, 'SEC Filings Show Hidden Ransomware Costs and Losses', *CSO Online*, 17 March 2022, <https://www.csoonline.com/article/572321/sec-filings-show-hidden-ransomware-costs-and-losses.html>, accessed 3 December 2023.

products or provide services to customers.[99] The high financial impact of business interruption was confirmed by a 2022 study of cyber insurance claims for ransomware that found that the average cost of business interruption amounted to $657,000.[100] Similarly, the interview data confirmed the significant financial harm caused by business interruption. One incident responder recalled working with manufacturing firms that were 'losing tens, if not hundreds, of millions of euros or pounds a day because … their manufacturing lines were flying [disrupted]'.[101] Business interruption also affected a victim in the charity sector, where the memberships team was unable to collect money from renewed membership subscriptions. As the annual direct debit collection was no longer working, the renewal process (worth £3 million) had to be delayed by a month.[102] Business interruption, including delayed payments, is thus not only a significant financial harm but can also lead to reputational harm if a victim is no longer able to provide their services. While there are generally few examples of organisations going out of business or facing insolvency solely due to a ransomware attack,[103] financial losses due to business interruption can be a significant influence in causing a business to shut down.

This factor is closely linked to financial harm caused by loss of expected income, for example where a victim organisation had to cancel several reservations for a venue it offers as a conferencing space.[104] Delay to another victim's project meant that an education institution was unable to secure funding for further related research.[105] Loss of expected income is of course closely related to the loss of clients. While often mentioned as a feared consequence, loss of clients is often difficult to directly attribute to the ransomware attack. An interviewee in the insurance business explained that although most insured parties do not lose a significant proportion of their customer base, this may happen in certain sectors (in the technology sector, for example, where customers display lower risk tolerance).[106] For organisations that provide immediate services, losing clients may be a more tangible harm, for example in the construction industry,

[99] For example, author interview with External Counsel 4, 1 March 2023; author interview with External Counsel 3, 21 December 2022, who described business interruption as being 'the most detrimental' element of ransomware attacks.

[100] Referring to the UK, the US and Canada. See NetDiligence, 'NetDiligence Cyber Claims Study', 2022, p. 5, <https://netdiligence.com/cyber-claims-study-2022-report/>, accessed 8 December 2023.

[101] Author interview with DFIR 2, 6 December 2022.

[102] Author interview with Charity 1, 12 January 2023.

[103] Alexander Martin, 'UK Logistics Firm Blames Ransomware Attack for Insolvency, 730 Redundancies', *The Record*, 26 September 2023, <https://therecord.media/knp-logistics-ransomware-insolvency-uk>, accessed 3 December 2023.

[104] Author interview with Charity 1, 12 January 2023.

[105] Author interview with Education 1, 8 December 2022.

[106] Author interview with Insurance Claims 1, 14 December 2022.

where the inability to provide a service would lead to the client immediately looking for a different supplier.[107]

Beyond the financial loss caused by loss of clients or expected income, ransomware attacks also result in a loss of time: the time that is needed to respond and recover. Ransomware attacks are highly disruptive, requiring the attention not just of IT staff but of staff from all departments. Financial harm also arises from time being spent responding to the ransomware attack, rather than on the usual tasks.[108] As a victim in the education sector said, 'The time cost is immense … The time cost of not only recovering, but not doing the work that you could have been doing'.[109]

Due to these financial losses and additional costs, interviewees widely regarded ransomware as a severe risk for organisations and potentially even as 'business ending … if you haven't got your data, you don't have a business'.[110] An executive of a micro-enterprise noted that they would have lost their house and their company would have gone bankrupt if they had not had the cushion of cyber insurance.[111]

While public reporting has highlighted some cases of organisations permanently ceasing to trade after a ransomware incident,[112] none of the victims interviewed reported that their organisation had ceased to be a going concern as the result of a ransomware attack. Interviewees from the ransomware recovery ecosystem (for example, incident responders and cyber insurers) were also hard-pressed to identify concrete cases where an organisation had ceased trading altogether. This may indicate a degree of selection bias: for example, organisations that were unable to afford incident response or did not have cyber insurance would not have been on these professionals' radar. The limited cases of this kind that interviewees could recall tended to relate to the healthcare sector – such as a fertility clinic holding highly sensitive data – where it was the combination of business interruption and irrecoverable reputational harm that resulted in the business folding.[113]

[107] Author interview with External Counsel 4, 1 March 2023.

[108] Author interview with Professional Services 1, 17 March 2023, especially on management time.

[109] Author interview with Education 3, 10 January 2023.

[110] Author interview with Technology 3, 24 March 2023; author interview with Technology 1, 20 March 2023; author interview with Local Government 2, 1 March 2023.

[111] Author interview with Consultancy 2, 17 March 2023.

[112] For example, see Catalin Cimpanu, 'Company Shuts Down Because of Ransomware, Leaves 300 Without Jobs Just Before Holidays', *ZDNet*, 3 January 2020, <https://www.zdnet.com/article/company-shuts-down-because-of-ransomware-leaves-300-without-jobs-just-before-holidays>, accessed 3 December 2023; Kevin Collier, 'An Illinois Hospital is the First Health Care Facility to Link its Closing to a Ransomware Attack', *NBC News*, 12 June 2023; in September 2023, it was reported that KNP logistics, the UK's largest logistics provider, declared insolvency as a result of a ransomware attack, see Martin, 'UK Logistics Firm Blames Ransomware Attack for Insolvency, 730 Redundancies'.

[113] Author interview with DFIR 7, 21 February 2023.

Reputational Harm

Alongside any financial impact, harm to their external reputation is often a primary concern for victim organisations.[114] Victims fear reputational harm arising either from media reporting or because customers and clients realise that the organisation is unable to provide a particular service. In some instances, victims have a contractual or regulatory – if not a moral – obligation to disclose that they have experienced a ransomware incident. Such incidents are, however, typically perceived as reflecting organisational weakness, and victims – who are also often subject to victim blaming – often fear that this will affect their reputation and professional credentials. A victim in the technology sector felt that 'we were humiliated in front of the customer',[115] while another victim, in the education sector, confirmed that their 'biggest bit of damage was probably reputational and confidence'.[116]

The driver behind such fear is the assumption that reputational harm in turn also leads to financial harm, for example due to loss of expected income or loss of clients.[117] One employee at a manufacturing company recollected that customers would repeatedly ask about the ransomware incident even months after the attack, and that rumours about customers' leaked personal data added to the reputational harm done.[118] As a result, the company was perceived as being less safe, and questions were raised about whether larger competitors were a safer choice for doing business with, indicating that this perception could have resulted in/contributed to a loss of orders.[119] Furthermore, the employee also noticed an impact on customer relations, as open communication with customers was prohibited, resulting in a feeling of lost trust among customers, who thought the employee knew more than they were telling.[120] This echoes a risk highlighted more widely in reporting on the subject: that, where there is an alternative supplier, the reputational fallout from a ransomware incident can include the loss of existing and future customers. In 2023, the hosting firms CloudNordic and AzeroCloud experienced ransomware attacks which irrevocably removed

[114] Reputational harm was also confirmed as a primary harm to organisations in author interview with Insurance Claims 3, 3 February 2023; author interview with DFIR 4, 14 December 2022.

[115] Author interview with Technology 1, 20 March 2023.

[116] Author interview with Education 4, 10 March 2023.

[117] Jeffrey Ton, 'Ransomware Damage: Are You Forgetting About Your Reputation?', *Forbes*, 8 April 2022, <https://www.forbes.com/sites/forbestechcouncil/2022/04/08/ransomware-damage-are-you-forgetting-about-your-reputation>, accessed 3 December 2023.

[118] Author interview with Manufacturing 1, 27 January 2023.

[119] *Ibid.*

[120] *Ibid.*

some hosted client data; the director of the companies said publicly that he did not expect many customers to remain with them.[121]

Reputational harm is often especially impactful for smaller firms providing professional services, particularly where there is an 'implied and contractual level of confidentiality' – for example, in legal or accountancy firms.[122] Customers perceive that it is part of these organisations' duty – but also their business model – to guard customers' personal information, which is often of a sensitive nature. In these instances, the disappointment and loss of trust increases the risk of reputational harm. Victim blaming after an attack can further aggravate reputational harm,[123] including via social media platforms.[124] While less pertinent for some of the interviewees at organisations that are less exposed to direct financial implications as a result of reputational damage (for example, because they are public sector organisations with no real competitors), reputational harm can thus have a significant impact on organisations.[125]

However, while the fear of reputational harm heavily influences victims' decision-making, some interviewees, including crisis communications experts and lawyers, indicated that reputational harm may not be as severe as has been assumed in the literature.[126] One interviewee did not think that there is 'stigma attached to being the victim of a cyber attack in the same way that there was in the past'.[127] Some victims said they had supportive clients or, in the case of schools and universities, students.[128] A victim in the professional services sector found that the attack 'did not do damage to our reputation as much as one might think, clients were quite sympathetic'.[129]

Nonetheless, the extent of reputational harm caused by a ransomware attack appears to be highly contingent and based on a range of factors. Some interviewees, for instance, highlighted that sympathy is likely to be dependent on the context of the incident and the nature of the business. One interviewee noted that their

[121] Claudia Glover, 'Devastating Ransomware Attack Hits Danish Cloud Hosting Companies CloudNordic and AzeroCloud', *Tech Monitor*, 25 August 2023, <https://techmonitor.ai/technology/cybersecurity/ransomware-attack-on-cloudnordic-azerocloud-loses-all-data>, accessed 3 December 2023.

[122] Author interview with DFIR 2, 6 December 2022.

[123] Author interview with Financial Services 1, 9 December 2022.

[124] Author interview with Insurance claims 2, 19 January 2023.

[125] See, for example, Heyburn et al., 'Analysis of the Full Costs of Cyber Security Breaches'; Ton, 'Ransomware Damage'.

[126] Aon and Pentland Analytics, 'Reputation Risk in the Cyber Age: The Impact on Shareholder Value', 2018, <https://www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf>, accessed 3 December 2023; Alena Yuryna Connolly and Hervé Borrion, 'Reducing Ransomware Crime: Analysis of Victims' Payment Decisions', *Computers and Security* (Vol. 119, Issue C, August 2022).

[127] Author interview with Insurance Claims 1, 14 December 2022.

[128] For example, the experience described in author interview with Education 2, 16 December 2022.

[129] Author interview with Professional Services 1, 17 March 2023.

inability to speak openly about the incident led to increasingly strained interactions with clients.[130]

Some interviewees also indicated that, if data exfiltration occurred, 'the risk of reputational harm is much greater'.[131] The same is true if customer services are interrupted. An interviewee at a professional services provider found that clients were 'reasonably sympathetic' as long as the company was still able to provide the relevant services and secure their data.[132] Other interviewees highlighted that the timing, cadence and tone of client communications was an important consideration for minimising harms to the organisation, its staff, clients and other third parties.[133] While each ransomware case will be different, it was emphasised that there was a balance to be struck between transparency and opacity, particularly with a public audience.[134] Such assessments are speculative, but again illustrate the prominence that the fear of reputational harm has for victims.

Another important finding from the interview data was that reputational damage can also occur within the impacted organisation itself. This is particularly likely where internal communication is poor, and especially among employees who are not directly involved in responding to the incident and who may, as a result, feel excluded. A victim in the professional services sector, who found that external reputational damage was not as significant as expected, said that the attack was indeed 'more damaging to our internal reputation',[135] adding that the attack's impact on morale made the organisation a bad place for people to work and that people were leaving as a result, with the organisation's reputation as an employer also suffering.[136]

Finally, victim organisations are often concerned about experiencing reputational harm as a result of media reporting. The interviewees for this project only mentioned a small number of examples of negative reporting in the media. Individual cases are not discussed here, given the risk of inadvertent attribution, but the interviews made clear that the fear of negative press often meant that victims – particularly those in the private sector – were less likely to be transparent about the attack. One victim spoke of negative publicity on social media.[137]

[130] Author interview with Manufacturing 1, 27 January 2023.

[131] Author interview with Insurance Claims 3, 3 February 2023. Also confirmed by author interview with External Counsel 4, 1 March 2023.

[132] Author interview with Professional Services 1, 17 March 2023.

[133] Author interview with Financial Services 1, 9 December 2022.

[134] Author interview with Financial Services 1, 9 December 2022; see also Richard Knight and Jason R C Nurse, 'A Framework for Effective Corporate Communication After Cyber Security Incidents', *Computers & Security* (Vol. 99, December 2020).

[135] Author interview with Professional Services 1, 17 March 2023.

[136] *Ibid*.

[137] Author interview with Financial Services 1, 9 December 2022.

First-Order Harms to Staff

In addition to the harm experienced by an organisation itself, the individuals who work for (or own) an organisation that has fallen victim to a ransomware attack are also directly impacted. As an interviewee in the charity sector put it, 'everyone was affected in a way, but just to different degrees'.[138] The degree to which staff members experience harm depends on a number of factors, including the extent to which they are involved in the immediate incident response and whether there are underlying issues, such as pre-existing health conditions. This section provides an overview of the different ways in which staff members may be negatively impacted by a ransomware attack, including psychological, physical, financial, reputational and social harm.

Psychological Harm

In contrast to public reporting, which often focuses on the financial harm of ransomware attacks, our interviews stressed that the first-order harm employees experience is primarily of a psychological nature. Interviewees repeatedly emphasised that psychological impacts are often overlooked in the wider discourse on ransomware attacks.[139]

Psychological impacts are naturally perceived at an individual level and are therefore highly subjective. The categories of psychological harm listed here are therefore not based on medical definitions but are guided by the interview data and by the words that individuals used to describe their feelings. Furthermore, psychological and physical harms are often closely interlinked, especially where psychological harm has physical consequences, such as mental burnout leading to tiredness or physical exhaustion. The distinction between the psychological and the physical is thus not always straightforward, but, to avoid duplication, not all harms are listed in both categories.

Primarily, experiencing and responding to a ransomware attack creates considerable stress for the individuals involved.[140] For example, an interviewee from the engineering sector confirmed, 'There's a huge amount of pressure and stress that everybody was under', to the extent that their company hired a post-traumatic stress disorder (PTSD) support team.[141]

[138] Author interview with Charity 1, 12 January 2023.

[139] For example, author interview with Insurance Claims 2, 19 January 2023; author interview with DFIR 5, 23 January 2023; author interview with DFIR 6, 1 February 2023.

[140] Author interview with DFIR 5, 23 January 2023; author interview with Professional Services 1, 17 March 2023; author interview with Engineering 1, 10 March 2023; author interview with DFIR 7, 21 February 2023.

[141] Author interview with Engineering 1, 10 March 2023.

While stress was widely reported, the interview data shows that individuals experience different forms of stress, depending on their position and allotted tasks. An interviewee in the professional services sector explained how management- and board-level employees felt stress due to financial concerns, while people in the middle management tier were stressed by the extremely long workdays, including particularly stressful communications with the threat actor.[142]

Stress is often particularly grave for individuals in involved IT teams.[143] One external service provider went so far as to state that 'the IT staff – they're the main victims of crime here'.[144] An interviewee from the education sector explained that the human toll on the IT service was especially severe due to their detailed understanding of the gravity of the situation, adding that the impact on the IT team was, however, often not talked about. As the technical details of attacks are often difficult to understand, the wider perception is that 'magical IT will come and sort it all out', obscuring how stressful this experience can be for the IT team.[145] Stress is also particularly prominent for IT teams because they feel a direct responsibility for protecting an organisation's systems.[146]

Although stress is thus often acknowledged as a harm inflicted by ransomware attacks, the interview data implied that the more detailed impact of stress, particularly on IT teams, is often overlooked and insufficiently addressed. This is particularly regrettable, as in some instances stress on staff is so significant that it leads to other harms such as burnout or other sickness, leading personnel to leave their jobs or to be absent temporarily on sick leave.[147]

Along with stress, victims also often described a feeling of confusion and loss of orientation in the initial phase of a ransomware attack, especially where victims were not familiar with technical details or did not yet have enough information to form a full picture of the situation. The loss of orientation may be rooted in there being insufficient preparation or procedures in place, while confusion can also stem from victims questioning why they have been attacked,[148] or from uncertainty among staff about what is going on and how they should respond.[149]

[142] Author interview with Professional Services 1, 17 March 2023.

[143] *Ibid.*; author interview with DFIR 5, 23 January 2023; author interview with Education 3, 10 January 2023.

[144] Author interview with DFIR 1, 5 December 2022.

[145] Author interview with Education 3, 10 January 2023.

[146] Author interview with Professional Services 1, 17 March 2023; author interview with DFIR 5, 23 January 2023.

[147] Author interview with DFIR 1, 5 December 2022.

[148] Author interview with Consultancy 2, 17 March 2023.

[149] Author interview with External Counsel 1, 12 December 2022.

As is the case for other categories of harm, victims noted that emotional reactions to ransomware attacks also varied with time. For example, a victim in the education sector said that 'those first few hours are quite horrific actually, until you get into a position where you start working out what the facts are'.[150] Others described feelings of very low mood in the first week after the attack.[151] One victim recalled a burdensome feeling that they 'for the foreseeable future belonged to the criminal underworld'.[152]

Some victims of ransomware attacks were also said to be angry, for example when an insurance provider recalled client interactions with victims who were angry at the attackers, questioning why they had been targeted.[153] Other interviewees said that former employees whose data was exfiltrated were also less sympathetic but 'much more angry'.[154]

Initial reactions of panic in the wake of a ransomware attack can also cause psychological harm.[155] One interviewee said 'there was a terror about what might happen next'.[156] On a related note, worry was a typical harm experienced by victims, for example worry about reputational risk,[157] but also, while responding to an attack, worry about whether they were taking the right actions. An external counsel noted that 'it's a harm in itself of distress and worry of making the wrong decision'.[158] A victim in the education sector spoke of a fear of recovering the IT systems too quickly, in case criminals still had access to the networks.[159] Fear of a repeated incident also affected other victims: when receiving suspicious emails or similar, even after the ransomware incident had been dealt with, victims experienced a sense of 'PTSD' (in the non-technical sense used by lay people), for example saying that 'there was a bit of a PTSD about every time I walked through the office door'.[160] Others described a sense of fear over potential job losses as a result of the ransomware attack.[161] These feelings underline how personally victims experience an attack, and how a ransomware incident casts a shadow over their personal and professional life.

The interviews revealed a number of further emotional harms that were experienced in response to ransomware attacks, stressing how wide-ranging

[150] Author interview with Education 3, 10 January 2023.
[151] Author interview with Consultancy 2, 17 March 2023.
[152] Author interview with Consultancy 2, 17 March 2023.
[153] Author interview with Insurance Claims 2, 19 January 2023.
[154] Author interview with Professional Services 1, 17 March 2023.
[155] Author interview with Local Government 2, 1 March 2023.
[156] Author interview with Consultancy 2, 17 March 2023.
[157] For example, author interview with Education 2, 16 December 2022.
[158] Author interview with External Counsel 1, 12 December 2022.
[159] Author interview with Education 3, 10 January 2023.
[160] Author interview with Consultancy 2, 17 March 2023.
[161] Author interview with DFIR 5, 23 January 2023.

the psychological impacts can be. The difficult decision about whether to pay the ransom demanded often weighs heavily on victims and is not a purely financial or risk management decision: it often raises feelings of guilt, an aspect often overlooked when considering the seemingly binary decision to pay or not to pay. A victim in the education sector described how challenging it was to make a decision in this context, given that they believed 'it's not ethical to pay the ransom'.[162] This concern had, however, to be balanced against students' potential delay to their studies. While the interviewee believed it was ultimately right to pay the ransom in this instance, they also stressed that 'we're not happy with the decision of paying'.[163]

Related to the feeling of guilt are feelings of shame and self-blame. An interviewee from the charity sector said 'we all blame ourselves' – a human reaction that was difficult to overcome.[164] Some members of IT teams can feel particularly responsible, often because they feel that they knew about potential system problems and did not raise them sufficiently, subsequently blaming themselves and burning themselves out working on the ransomware response.[165] Again, this underlines the overlooked – but heightened – impact that ransomware attacks have on the mental wellbeing of IT teams in particular.

Interviews also highlighted that ransomware attacks caused feelings of doubt and resignation among victims, again underlining how personal the attack is felt to be by its victims. One interviewee said the incident made them doubt everything they had done.[166] Similarly, another interviewee said that the incident made them question whether they had run their business properly, because 'at that time you second guess yourself, [and] that adds to the mental anxiety'.[167] Another victim described a sense of doubt about whether they were doing enough, but also a feeling of resignation 'to the fact that if someone wants to get in [and] if they have enough time and enough energy and enough effort – they'll get in'.[168]

Recent research shows that the range of psychological harm experienced, and its severity, can affect victims' mental health.[169] Indeed, interviewees overwhelmingly felt that this aspect was often overlooked in popular discourse.

[162] Author interview with Education 1, 8 December 2022.

[163] *Ibid*.

[164] Author interview with Charity 1, 12 January 2023.

[165] Author interview with DFIR 1, 5 December 2022.

[166] Author interview with Consultancy 2, 17 March 2023.

[167] Author interview with Consultancy 3, 17 March 2023.

[168] Author interview with Charity 1, 12 January 2023.

[169] Ryan Shandler and Miguel Gomez, 'The Hidden Threat of Cyber-Attacks: Undermining Public Confidence in Government', *Journal of Information Technology and Politics* (Vol. 20, Issue 4, September 2022); Ryan Shandler, Michael L Gross and Daphna Canetti, 'Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis', *Journal of Global Security Studies* (Vol. 8, Issue 1, March 2023).

One victim concluded that 'the overall piece is that we very rarely talk about the mental health impact of these events'.[170]

Like other categories of harm, psychological harm continues far beyond the immediate timeframe of the incident, creating an additional mental health burden and making it challenging for victims to move on after the incident. Victims repeatedly mentioned concerns over the role of the Information Commissioner's Office and the impact that the prospect of being fined had on their mental state.[171] The challenge of moving on mentally after an incident was also reported by an interviewee in the education sector, who said that subsequent Ofsted surveys revealed that 'some staff are still very raw about this. When you ask them about workload, they may well say the ransomware attack … made our lives hell'.[172] Another victim felt 'a real disappointment' given that their company was ultimately unable to find out how the attacker gained access to their systems.[173] Indeed, one victim went as far as to say that the attack made them feel like they had 'failed'.[174] Another victim found the ransomware attack 'actually really traumatic' (especially given their strong identification with success in business, and in their own business in particular), indicating that this had brought them close to suicide.[175]

Interview data shows that not only is the psychological impact of ransomware incidents overlooked in the short term, but that the long-term psychological impact of attacks is even less likely to be noticed (or sufficiently addressed) than immediate harms such as stress.

While the psychological harm a ransomware attack causes is of course highly context specific and also depends on the individuals involved and their existing mental health conditions, the interviews stressed the significance, extent and multiplicity of ways in which victims experience psychological harm. Such psychological harm can reach far beyond the immediate response to a specific incident, affecting an individual's wider professional life and impacting their personal life. Interviewees repeatedly noted that the psychological impact of ransomware attacks is insufficiently recognised, not only by the broader public, but also in academic and/or industry studies and within the organisations responding to such attacks.[176]

[170] Author interview with Engineering 1, 10 March 2023.

[171] Author interview with Consultancy 2, 17 March 2023.

[172] Author interview with Education 4, 10 March 2023.

[173] Author interview with Engineering 1, 10 March 2023.

[174] Author interview with Education 2, 16 December 2022.

[175] Author interview with Consultancy 2, 17 March 2023.

[176] For an example of an analysis of the psychological impacts of broad cybercrime, see Alexa Palassis, Craig Speelman and Julie Pooley, 'An Exploration of the Psychological Impact of Hacking Victimisation', *Sage Open* (Vol. 11, No. 4, November 2021).

The research data demonstrates how central the psychological impact is to victim experience and how varied the psychological harm is, especially for IT teams. In turn, such psychological impact on individuals also has financial impact for victim organisations, for example where it affects productivity, when staff suffer burnout and need replacing, or in terms of other forms of employee turnover.

Physical Harm

Victims' physical health also suffers in the wake of ransomware attacks. Physical harms reported by interviewees ranged from minor ailments (for instance, weight changes) to serious health issues (such as heart attack or stroke). While not a commonplace occurrence, one law enforcement interviewee noted that they knew of a member of IT staff at an organisation who took their own life following a ransomware incident.[177] Far more commonly, interviewees reported sleep deprivation and follow-on impacts, with employees falling asleep at the office[178] or reporting problems sleeping at home.[179] One victim reported that 'the fatigue on people was extreme', referring to physical but also mental exhaustion, illustrating how closely linked the two harms are.[180] This is also true for harms such as burnout, which can manifest in both mental and physical ways. Other reported physical impacts included weight loss[181] and dehydration.[182]

One interviewee even reported health issues within their team that resulted in hospitalisation, with employees not looking after themselves well in the immediate response to a ransomware attack, for example by drinking too much coffee and not enough water (which in this instance resulted in the need for hospital checks because of pre-existing heart complications).[183] In a more grievous example, a victim experienced a heart attack and required surgery, citing the stress of managing the incident as a key factor.[184] Physical harm is thus closely linked to the mental harm experienced, such as stress and anxiety; this can be especially grave where victims have underlying health conditions (albeit this is the exception rather than the rule).

[177] Author interview with Law Enforcement 1, 9 December 2022; author interview with Ransomware Specialist 1, 12 December 2022.
[178] Author interview with Engineering 1, 10 March 2023.
[179] Author interview with Consultancy 2, 17 March 2023.
[180] Author interview with Technology 1, 20 March 2023.
[181] Author interview with Consultancy 2, 17 March 2023.
[182] Author interview with Charity 1, 12 January 2023.
[183] *Ibid*.
[184] Author interview with Financial Services 1, 9 December 2022.

Financial Harm

While wider reporting of ransomware incidents often focuses on the financial impact for organisations or the economy more broadly, the interview data stresses that financial harm is also experienced by individual staff members. (The distinction is, of course, somewhat superfluous in the case of sole traders or freelancers, whose individual financial situation is hardly distinguishable from that of their business.)

Employees can suffer financial harm as a result of a ransomware attack, for example if they lose their job as a result of the attack – an outcome that is more likely for members of the IT team or an organisation's board members. An external counsel reported that, especially where a publicly listed company pays the ransom, board members are likely to be changed within six months to a year.[185]

While many victims reported that their organisation was still able to meet payroll despite the ransomware attack, this was often because the incident came just after staff had been paid, or otherwise that it had been a close call with regard to meeting payroll during response to the incident. Not being paid, or being underpaid (for example, because a recent pay rise has been ignored due to fallback to earlier backups of personnel data), is thus another way in which a ransomware attack can financially impact staff members.[186] Another example of harm was described by one victim, who paid for their own therapy sessions (which were not covered by insurance) and had to cancel holiday plans in order to make time to respond to an attack.[187]

Reputational Harm

Like organisations, individual staff members may also be concerned about suffering reputational harm as the result of a ransomware attack. This is particularly true for IT staff, who often feel that they may not have done enough to prevent the incident from occurring. They might also be blamed by board members or other senior staff for not doing what might superficially be considered 'doing their job'.

Reputational harm is also a problem for staff who might have clicked on a malicious link (allowing ransomware to access the organisation's systems) or whose credentials have been abused during the attack. Even if they were not

[185] Author interview with External Counsel 3, 21 December 2022.

[186] Author interview with DFIR 7, 21 February 2023; author interview with Foreign Government 1, 22 November 2022.

[187] Author interview with Consultancy 2, 17 March 2023.

necessarily responsible for the breach, their reputation might suffer if they are erroneously assigned blame by superiors or colleagues.[188] Blaming individuals and contributing to their reputational harm might also cause them further psychological harm.

Social Harm

In addition to the psychological, physical and financial harm caused, a ransomware attack can also impact employees' professional lives, and the social relations between members of staff, and their relationships outside work.

For example, the psychological harm experienced by staff members can have wider impacts on social relations within an organisation or team, potentially leading to strained relationships with colleagues.[189] One victim described employees as being 'grumpier', amid increased workloads and diminished pastoral care.[190] Others noted the negative effect on morale and said that the repeated complaints of colleagues were 'annoying'.[191] Work relationships might also become strained if external help is hired. One victim described how the in-house IT team felt challenged when an external IT team was hired as additional help, with poor integration leading to duplication of efforts and resources.[192]

The impact of ransomware attacks is, however, also felt beyond social relations in a professional context, extending into private and family life. Some victims reported missing out on personal or family life.[193] One victim described 'a personal toll', particularly given increased commuting demands and long working hours.[194] The impact on personal life was also felt by a victim in the technology sector who described a 'work–life balance loss through extended hours of working weekends'.[195] Another interviewee, who coordinated incident response, described how he personally provided impromptu childcare for one of their chief IT technicians, so that the technician could be 'hands-on-keyboard'.

Those staff members who are not part of an organisation's 'core' ransomware response team also experience harm to their professional and private lives, although the nature of the harm may differ from that of those forming part of the 'inner circle'. Those outside the immediate response team might feel 'like

[188] Author interview with DFIR 1, 5 December 2022; author interview with DFIR 6, 1 February 2023; author interview with Outsourcing 1, 15 December 2022.

[189] Author interview with Insurance Claims 2, 19 January 2023; author interview with Professional Services 1, 17 March 2023; author interview with Manufacturing 1, 27 January 2023.

[190] Author interview with Professional Services 1, 17 March 2023.

[191] Author interview with Manufacturing 1, 27 January 2023.

[192] Author interview with Professional Services 1, 17 March 2023.

[193] For example, author interview with Engineering 1, 10 March 2023.

[194] Author interview with Charity 1, 12 January 2023.

[195] Author interview with Technology 1, 20 March 2023.

really nobody had a handle on it' and feel left out of the communication loop, receiving little information about what is going on.[196] Understandably, there is also a degree to which professional and personal life entwine, particularly where staff pursue their work as a personal passion. Interviewees also noted that some staff treated the ransomware attack as an opportunity – or impetus – to resign from their role or take retirement; for instance, educational staff who had lost many years' worth of teaching materials.[197] Another interviewee noted that staff who had been with their organisation for decades felt a form of 'love' towards the archives of data that they had personally collected during their career, and felt bereft at the loss of this data.[198]

Many staff members experience different degrees of ransomware harm, which in turn have negative impacts on their professional and private lives. Such negative impacts are closely tied to the psychological impact staff members experience, again demonstrating the interconnectivity of harms – as well as the wide range of forms that psychological harm can take.

This section has illustrated the categories of harm experienced by direct victims of ransomware attacks: that is, the organisations and staff members who experience the ransomware attack. Organisations face potential digital/physical, financial and reputational harm, while staff members may encounter financial, reputational, psychological, physical and social harm. Importantly, though, harm is also felt beyond these first-order harms, extending to those who indirectly experience harm as a result of a ransomware attack. The following sections illustrate what these second- and third-order harms can look like.

Second-Order Harms

The second category of harms involves organisations and individuals indirectly harmed by ransomware. The former group includes organisations that are customers/clients or in the supply chain of a victim entity that has had its IT systems encrypted or data stolen, while the latter group – individuals – refers to the customers or users of a public or private organisation that provides services or holds data.

The research conducted for this paper highlights that, the further 'downstream' we get from the initial impact of the attack, the more challenging it is to effectively characterise and illustrate harms to organisations.[199] However, the research has

[196] Author interview with Manufacturing 1, 27 January 2023.

[197] Author interview with Education 2, 16 December 2023.

[198] Author interview with Government Agency 2, 3 March 2023.

[199] Nandita Pattnaik et al., 'It's More Than Just Money: The Real-World Harms from Ransomware Attacks', in S Furnell and N Clarke (eds), *Human Aspects of Information Security and Assurance*, IFIP Advances in

been able to identify a range of second-order harms to organisations and individuals through the interviews with direct victims, third-party experts and law enforcement, and via academic literature and media reporting. The results of a ransomware-harm modelling exercise conducted as part of this project and published as an academic conference paper have also been important in highlighting the different types of harms that can indirectly affect individuals, particularly healthcare patients and residents of local authorities that are affected by ransomware.[200]

Taken together, the various types of second-order harms from ransomware operations help emphasise their long tail and wide reach, shedding light on the various ways in which individuals are impacted by ransomware attacks. Ransomware attacks that disrupt the operations of businesses and public services have cascading effects that harm the lives of citizens of the UK and many other countries.

Information and Communication Technology, Vol. 674 (Cham: Springer, 2023), pp. 261–74, <https://doi.org/10.1007/978-3-031-38530-8_21>, accessed 3 December 2023.

[200] *Ibid.*

Figure 4: Types of Second-Order Harms Affecting Downstream Organisations and Individuals

Organisations	Individuals		
Digital/physical/financial/reputational/psychological (organisations and their staff downstream from first-order victims may experience the same harms)	Physical harm	Financial harm	Psychological harm
	Patient care disrupted	Payment of benefits disrupted	Stress
	Elective surgeries disrupted	Housing sales disrupted	Anxiety
	Increased waiting times	Price increases	Fear
	Risk to physical safety from disruptions to emergency services	Extorted for additional ransom payments	Frustration
	Housing conditions deteriorating due to local government backlogs	Identity theft/fraud	Confusion
	Increased physical risk to vulnerable individuals due to data leaks		Anger
			Shame
			Panic
			Lack of access to mental health services due to disruption

Source: Author generated.

Second-Order Harms to Organisations

As illustrated in Figure 4, ransomware operations have the potential to create a range of second-order harms for organisations and their employees, even when they are not directly targeted.

Ransomware attacks on outsourced IT services, such as managed service providers or cloud hosting providers, can harm organisations' digital systems and data. A 2022 ransomware operation against Rackspace Technology, a cloud hosting provider, encrypted Microsoft Exchange email servers and caused thousands of SMEs to lose access to email services for several days.[201] A more recent ransomware attack against CloudNordic, a cloud services provider, resulted in customers losing all their data after the company's backups were deleted.[202]

Disruptions to organisations' supply chains and subsequent harms are not limited to ransomware attacks on technology providers. Nor are they a rare exception, with data indicating that 52% of firms say that one of their suppliers has experienced a ransomware attack.[203] Physical supply chains can be particularly sensitive to ransomware harm: attacks against organisations in sectors such as manufacturing and logistics can create cascading effects that spread financial and reputational harm down the supply chain as suppliers and customers experience delays and loss of trust.[204] One interviewee from the manufacturing sector, for example, highlighted how a ransomware attack against their company resulted in delays to their customers' operations; in some cases, this resulted in customers finding new suppliers.[205] Interviews also highlighted that being downstream from a ransomware attack can be even more challenging than being at the epicentre, as access to information about the attack may be much more limited.[206] As a breach response lawyer argued, second-order harms may be 'in a way, slightly worse, because you're reliant on [the organisation experiencing the ransomware attack] for information … but they're not going to be able to give you complete information in the early stages'.[207] In some cases, suppliers experiencing ransomware attacks may even attempt to pretend the ransomware attack is not happening in an effort to reduce their own reputational harm.[208]

In this sense, first- and second-order harms are not discrete – rather, they are closely linked. Severe second-order harms are likely to multiply the extent of

[201] Jai Vijayan, 'Rackspace Incident Highlights How Disruptive Attacks on Cloud Providers Can Be', *Dark Reading*, 7 December 2022, <https://www.darkreading.com/cloud/rackspace-incident-highlights-disruptive-attacks-on-cloud-providers>, accessed 5 December 2023.

[202] Zack Whittaker, 'Danish Cloud Host Says Customers "Lost All Data" After Ransomware Attack', *Tech Crunch*, 23 August 2023, <https://techcrunch.com/2023/08/23/cloudnordic-azero-cloud-host-ransomware/>, accessed 5 December 2023.

[203] Trend Micro, 'Everything is Connected: Uncovering the Ransomware Threat From Global Supply Chains', January 2023, <https://www.trendmicro.com/explore/glrans>, accessed 5 December 2023.

[204] Nicolas Rivero, 'Ransomware Hackers are Now Going After Supply Chain Companies', *Quartz*, 23 February 2022, <https://qz.com/2132444/ransomware-hackers-are-now-going-after-supply-chain-companies>, accessed 5 December 2023; Matteo Crosignani, Marco Macchiavelli and André F Silva, 'Pirates Without Borders: the Propagation of Cyberattacks Through Firms' Supply Chains', *Journal of Financial Economics* (Vol. 147, Issue 2, February 2023), pp. 432–48.

[205] Author interview with Manufacturing 1, 27 January 2023.

[206] *Ibid*.; author interviews with Crisis Communications 1 and DFIR 2, 6 December 2022.

[207] Author interview with External Counsel 2, 14 December 2022.

[208] Author interview with Manufacturing 1, 27 January 2023, who recounted that they were told not to tell customers about their ransomware attack.

harm or pressure on the direct victim organisation. For instance, an insurance claims handler recalled supporting an industrial system supplier to the fast food industry.[209] The victim emphasised to the interviewee that their clients had zero tolerance for downtime; kitchens were supposed to be operating at full capacity in a context where fryers and other equipment would routinely break down, warranting rapid repair.[210] If the victim could not return to operations within a matter of hours or days, they would be 'booted off' contracts worth millions of pounds.[211]

It is also increasingly common for organisations to have data stolen by ransomware threat actors via their suppliers' systems. When Capita, a major provider of outsourced IT services in the UK, was targeted by cyber-criminals using BlackBasta ransomware, more than 90 of its customers had data stolen.[212]

Listing all the various potential types of financial, reputational, physical, psychological and social second-order harms to organisations and their employees from ransomware is beyond the scope of this paper, given that the interviews and workshops focused predominantly on the experiences of direct victims. However, it is reasonable to conclude that second-order harms may take a similar form to the first-order harms listed in the previous section, since they ultimately stem from disruption to business operations and the theft of data. In this sense, the harms experienced by third parties can be comparable to those experienced by the direct victim (rather than being seen as vicarious nuisance). As one breach response lawyer articulated, 'If you're reliant on someone that has an incident, you can't do business as a result of their incident, then clearly you're in a pretty similar position in a way, insofar as you may not be able to do business properly'.[213]

Second-Order Harms to Individuals

Ransomware also creates a range of second-order harms – some of which are sector specific – for individuals downstream from the initial victim. Here, the term 'individuals' refers to customers or users of goods and services, including people from groups such as hospital patients or schoolchildren. Given the digital dependencies of most businesses and service providers in modern economies and societies, individuals have significant exposure to ransomware harms. This paper's research shows that individuals who are already vulnerable, such as

[209] Author interview with Insurance Claims 3, 3 February 2023.
[210] *Ibid.*
[211] *Ibid.*
[212] Joanna Partridge, 'Cyber Attack to Cost Outsourcing Firm Capita Up to £25m', *The Guardian*, 4 August 2023.
[213] As highlighted in author interview with External Counsel 2, 14 December 2022.

patients seeking medical treatment or people receiving benefits, are disproportionately impacted by the indirect harm caused by ransomware attacks.

Physical Harm

There is a growing body of evidence that ransomware causes downstream harm to the physical health of individuals, most significantly when such harm reduces health outcomes at hospitals after attacks. Many ransomware groups have been ruthless in directly targeting hospitals and healthcare providers, showing scant regard for the impact on essential services and patients.[214]

As the attack on Ireland's Health Service Executive (HSE) by the Conti ransomware group illustrates, the disruption of IT services can cause cascading harms to clinical services and patients. Attacks against hospitals have forced elective surgeries to be cancelled and disrupted patient services such as cancer treatments.[215] During the HSE attack, for instance, radiation therapy stopped at five centres, while 513 patients had their cancer treatment disrupted.[216] In other cases, ransomware attacks have caused emergency services to be diverted to other hospitals;[217] in critical care services, where minutes or hours can determine whether a patient lives or dies, these kinds of diversions can reduce survivability and recovery.[218] One recent report has suggested that between 2016 and 2021, between 42 and 67 Medicare patients in the US died as a result of ransomware incidents,[219] while several surveys and studies indicate that ransomware attacks

[214] Author interview with DFIR 1, 5 December 2022; author interview with DFIR 3, 12 December 2022; author interview with DFIR 5, 23 January 2023; author interview with DFIR 7, 21 February 2023.

[215] Mihir Bagwe, 'Ransomware Attack Disrupts Japanese Hospital for 2nd Day', *Bank Info Security*, 2 November 2022, <https://www.bankinfosecurity.com/ransomware-attack-disrupts-japanese-hospital-for-2nd-day-a-20397>, accessed 5 December 2023; Kari Paul, '"Lives Are at Stake": Hacking of US Hospitals Highlights Deadly Risk of Ransomware', *The Guardian*, 14 July 2022.

[216] PWC, 'Conti Cyber Attack on the HSE: Independent Post Incident Review', 3 December 2021, p. 15, <https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>, accessed 5 December 2023; Aileen Flavin et al., 'A National Cyberattack Affecting Radiation Therapy: The Irish Experience', *Advances in Radiation Oncology* (Vol. 7, No. 5, September–October 2022).

[217] Dan Goodin, 'Hospitals Hamstrung by Ransomware are Turning Away Patients', *Arstechnica*, 16 August 2021, <https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/>, accessed 5 December 2023; Livi Stanford, 'Hospital Shaken by Attack: Patients Diverted to Saint Mary's as Computers Impacted', *Republican American*, 7 August 2023, <https://www.rep-am.com/localnews/2023/08/07/hospital-shaken-by-attack-patients-diverted-to-saint-marys-as-computers-impacted/>, accessed 5 December 2023; Johana Bhuiyan, 'Cyberattack Disrupts Hospital Computer Systems Across US, Hindering Services', *The Guardian*, 4 August 2023.

[218] Cybersecurity and Infrastructure Security Agency (CISA), 'Provide Medical Care is in Critical Condition: Analysis and Stakeholder Decision Support to Minimize Further Harm', *CISA Insights*, September 2021, <https://www.cisa.gov/sites/default/files/publications/Insights_MedicalCare_FINAL-v2_0.pdf>, accessed 5 December 2023.

[219] Claire McGlave, 'Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients', *SSRN*, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292>, accessed 8 December 2023.

are linked to increased mortality rates at affected hospitals.[220] In a recent survey of healthcare professionals in the US by the Ponemon Institute, for example, 24% of respondents said their hospital experienced an increase in excess deaths following a ransomware attack.[221]

Other effects may be less noticeable, but nevertheless still degrade the quality of care individuals receive. Losing access to electronic health records, for instance, forces doctors and nurses to revert to pen and paper; this reduces productivity, which in turn limits the number of patients that can be treated.[222] In the longer term, patients whose detailed records inform choices about their treatment receive less effective care if those records are inaccessible or corrupted.[223]

Ransomware can affect individuals' physical health even if their healthcare provision is not disrupted. The attack on Hackney Council, for example, contributed to delays in repairs to social housing stock. According to reporting, one resident's home suffered damp, mould and leaks after the council lost access to records about the property.[224] Disruptions to the provision of social care can also cause physical harms: a disabled resident in Hackney told a journalist that the ransomware attack had prevented her from accessing social care services for several months – 'I could not wash myself. I couldn't wash my own hair'.[225] These examples highlight how ransomware attacks against local government entities can be particularly harmful, due to the range of basic services these entities provide, further emphasising that it is the already vulnerable who are disproportionately affected by the second-order harms caused by ransomware attacks. Policymakers must consider what policy measures can be taken to protect these vulnerable people from such harm.

In extreme circumstances, the exfiltration and release of data also has the potential to expose individuals to varying degrees of personal physical risk. This stems from an emergent trend in which ransomware operators exfiltrate data from organisations that hold highly sensitive personal data – for instance, schools and law firms.[226] A severe example highlighted in interviews was the possible doxing of relocated domestic abuse survivors following the theft of data

[220] Ponemon Institute, 'Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care', <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>, accessed 5 December 2023; CISA, 'Provide Medical Care is in Critical Condition'.

[221] Cynerio, 'Cynerio and Ponemon Study Finds Frequent Cyber Attacks and Insufficient Accountability in Healthcare Adversely Impact Patient Care', *PR Newswire*, 15 August 2022, <https://www.prnewswire.com/news-releases/cynerio-and-ponemon-study-finds-frequent-cyber-attacks-and-insufficient-accountability-in-healthcare-adversely-impact-patient-care-301604539.html>, accessed 5 December 2023.

[222] PWC, 'Conti Cyber Attack on the HSE'.

[223] CISA, 'Provide Medical Care is in Critical Condition'.

[224] Burgess, 'The Untold Story of a Crippling Ransomware Attack'.

[225] *Ibid*.

[226] Bajak, Hollingsworth and Fenn, 'Ransomware Criminals are Dumping Kids' Private Files Online After School Hacks'; John Hyde, 'Firm Fined Almost £100,000 Over Ransomware Attack', *Law Gazette*, 10 March

from a law firm; the malicious public release of such data could put such individuals and those around them at extreme personal risk.[227] An interviewee from the education sector recalled feeling relief when they realised that the ransomware operators involved in their attack had gained access to commercial data – including payroll – but did not get access to pupil safeguarding data.[228]

Financial Harm

Ransomware also has the potential to harm individuals financially. In some cases, second-order financial harm can stem from disruption to particular financial services or goods; or, in a small number of cases, from the risks associated with stolen and leaked personal financial information.

In the UK, ransomware operations against local authorities have disrupted residents' ability to access housing benefits, again disproportionately impacting those who were already vulnerable. One senior leader at a council described the 'massive disruption' to local residents, recounting that 'people couldn't pay their rent'.[229] Hackney Council's housing benefit services were also significantly impacted,[230] and in July 2022 a news report suggested that a family of seven living in Hackney had been forced to leave their home because the council was unable to update their housing benefit payments.[231] A UK law enforcement officer said that disruptions to state benefits 'might stop [residents] being able to put food on the table for their kids'.[232] Critically for policymakers, these examples highlight how personally ransomware attacks are experienced, and how already vulnerable groups are disproportionately affected by them – problems that require nuanced consideration when designing policy responses.

More intangible are the potential downstream impacts from ransomware attacks on the costs of goods and services for individual consumers. Although this research did not uncover specific evidence of price rises for consumers following ransomware attacks, a study by IBM highlights that 62% of firms affected by ransomware raised their prices in the aftermath.[233] It is reasonable to expect

2022, <https://www.lawgazette.co.uk/news/firm-fined-almost-100000-over-ransomware-attack-/5111806.article>, accessed 5 December 2023.

[227] Author interview with Law Enforcement 1, 9 December 2022; author interview with DFIR 7, 21 February 2023.

[228] Author interview with Education 2, 16 December 2022.

[229] Author interview with Local Government 2, 1 March 2023.

[230] Burgess, 'The Untold Story of a Crippling Ransomware Attack'.

[231] Sam Holder, 'UK Councils and Hospitals at Risk of Cyber Hackers, ITV News Reveals', *ITV News*, 5 July 2022.

[232] Author interview with Law Enforcement 1, 9 December 2022.

[233] IBM, 'Cost of a Data Breach Report 2022', <https://www.ibm.com/downloads/cas/3R8N1DZJ>, accessed 5 December 2023.

that some price rises may be directly felt by individuals, particularly for consumer-facing services.

There is also a small possibility that individuals whose personal data is stolen by ransomware operators may be personally extorted or defrauded by other cyber-criminals in the ransomware ecosystem. On a small number of occasions, threat actors have tried to personally extort individuals whose data has been stolen as part of a ransomware operation, the most notable example being the theft of healthcare data from a Finnish therapy provider by cyber-criminals, who then also extorted patients.[234] However, interviewees highlighted that this example is likely to be the exception rather than the rule.[235]

An insurance claims interviewee recalled an attack on a private school, wherein the ransomware operators directly contacted pupils' parents before delivering the ransomware payload.[236] These fraudulent emails offered parents a 10% discount on forthcoming school fees if the parents made an expedited payment (to a false payment address).[237] This reflects the relatively new ransomware attack model of 'triple extortion', wherein the threat actors not only encrypt and exfiltrate data held by the direct victim organisation, but also target secondary parties (clients) to solicit additional payments.[238]

Media reports on ransomware, particularly incidents involving large stolen datasets, often speculate that stolen and leaked personally identifiable information and financial details might be used for identity theft and fraud.[239] However, the research conducted for this paper suggests that ransomware operators or other cyber-criminals are not monetising stolen personal data in a systematic way. Interviewees and workshop participants from incident response, law firms and law enforcement all emphasised there is little evidence that ransomware operators are cleaning and aggregating stolen data in a way that would allow them to sell it to other cyber-criminals or use it for financial fraud.[240]

[234] William Ralston, 'They Told Their Therapists Everything. Hackers Leaked It All', *Wired*, 4 May 2021, <https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/>, accessed 5 December 2023; Alex Scroxton, 'Hacked Finnish Therapy Business Collapses', *Computer Weekly*, 11 February 2021, <https://www.computerweekly.com/news/252496227/Hacked-Finnish-therapy-business-collapses>, accessed 5 December 2023.

[235] Author interview with Ransomware Specialist 1, 12 December 2022; author interview with Ransomware Specialist 3, 7 March 2023; author interview with Law Enforcement 1, 9 December 2022; author interview with External Counsel 3, 21 December 2022; author interview with DFIR 2, 6 December 2022.

[236] Author interview with Insurance Claims 3, 3 February 2023.

[237] Author interview with Insurance Claims 3, 3 February 2023.

[238] Cyber insurance claims manager, November 2022 workshop.

[239] *BBC News*, 'Cyber Attack: Data from Charities Stolen in Ransomware Attack', 17 April 2023; Kevin Collier, 'Hackers are Leaking Children's Data – And There's Little Parents Can Do', *NBC News*, 10 September 2021.

[240] Author interview with DFIR 2, 6 December 2022; author interview with DFIR 7, 21 February 2023; author interview with Ransomware Specialist 3, 7 March 2023; author interview with External Counsel 3, 21 December 2022; author interview with Law Enforcement 1, 9 December 2022; author interview with Law Enforcement 2, 13 December 2022.

There are likely several reasons why ransomware criminals do not currently exploit stolen data for further criminal gains. First, for the time being, it is simply much more profitable for criminals in the ransomware ecosystem to engage in or enable extortion-based crimes.[241] Second, it is costly and time consuming to host, clean and aggregate stolen data in a way that would be useful and monetisable. A ransomware negotiator noted that a personal record for an individual was likely to be worth between $1 and $4, thus offering limited profitability unless the dataset was ordered in a readily hostable and saleable format.[242] The saleability of such data is also likely to be hampered by the cost of server storage and the unreliability of darknet-hosted platforms.[243] As a lawyer involved in breach response explained, lawyers and forensic experts often take weeks or months (with the use of specialist software) trying to figure out what type of data has been stolen during a ransomware incident, a process which cyber-criminals are unlikely to have the resources or inclination to emulate.[244]

Taken together, these factors suggest that the potential financial harm to individuals from data stolen by ransomware threat actors is not as significant as many people believe. While policymakers must be aware that further extortion from leaked data is a possibility, this impact should not be overestimated, although this should certainly not distract attention from the concrete psychological harm that victims experience (and which is currently often overlooked). However, this does not rule out cyber-criminals or other threat actors exploiting this data in the future, particularly if technological changes enable them to aggregate it more efficiently.

Psychological Harm

Ransomware can also cause psychological harm to individuals who are not involved with the immediate response or who do not work for the targeted organisation. Although the research conducted for this paper does not include interviews with victims from outside (direct) victim organisations, other sources such as media reporting, academic literature and our interviews with subject matter experts illustrate some of the negative impacts from ransomware on individuals' mental health and wellbeing.

First, ransomware attacks that cause downtime for essential services like healthcare, local government and education can cause stress, anxiety, confusion and fear for the individuals who use these entities' services. Beyond the immediate

[241] Author interview with Ransomware Specialist 3, 7 March 2023.

[242] *Ibid.*

[243] *Ibid.*

[244] Author interview with External Counsel 3, 21 December 2022; see also author interview with Ransomware Specialist 3, 7 March 2023.

impact on physical health stemming from ransomware attacks on healthcare services, the mental health effects on patients and families have also been made clear in news coverage.[245] Delays to important test results or outpatient services like cancer treatments or elective surgeries can cause distress and anxiety for patients and their families, as the attack against HSE illustrated. The interruption of local government services such as social care, housing and child benefits, and council housing can also lead to stress and even anger among affected residents.[246]

Second, the rise of double-extortion ransomware operations has created additional psychological harms for individuals whose data has been stolen and leaked.

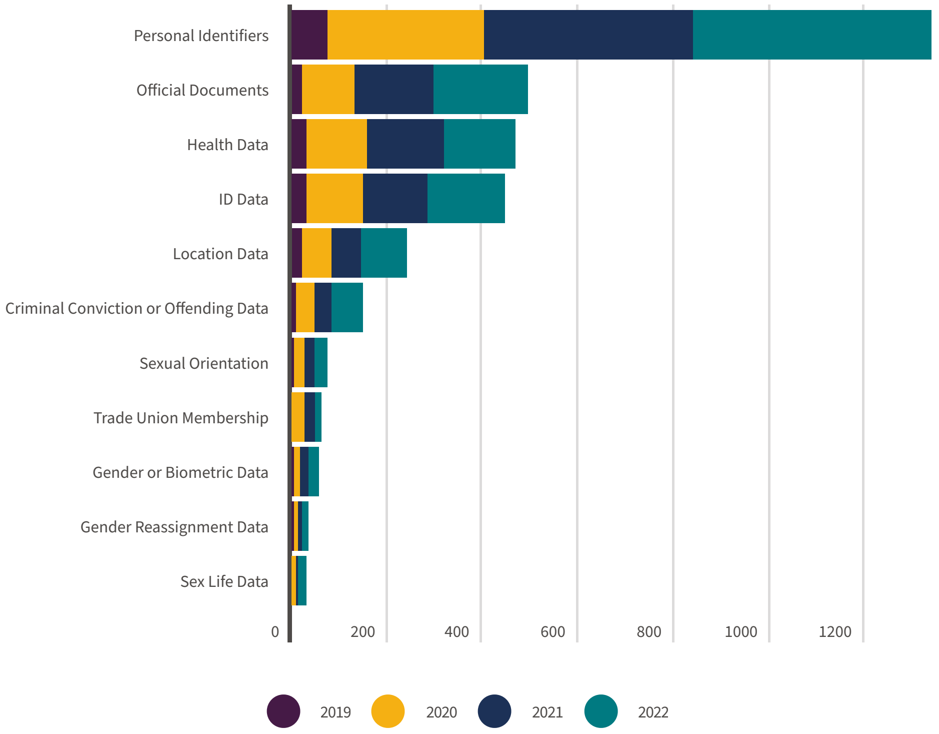
Although the concrete risk of fraud and identify theft related to data stolen by ransomware threat actors appears to be low, this is not the dominant public perception. As one incident response practitioner suggested, ‘you can’t necessarily reassure [people] who, through no fault of their own, have had all of their details compromised’.[247]

[245] Kevin Collier, ‘Ransomware Attacks on Hospitals Take Toll on Patients’, *NBC News*, 8 November 2022; Mark Stockley, ‘A Doctor Reveals the Human Cost of the HSE Ransomware Attack’, MalwareBytes, 20 May 2021, <https://www.malwarebytes.com/blog/news/2021/05/a-doctor-reveals-the-human-cost-of-the-hse-ransomware-attack>, accessed 5 December 2023.

[246] Author interview with Local Government 2, 1 March 2023.

[247] Author interview with DFIR 7, 21 February 2023.

Figure 5: Ransomware Incidents Involving Exposure of Personal Data



Source: 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 11 January 2024.

As highlighted in Figure 5, a range of personal data can be impacted by ransomware incidents. When particularly sensitive data, such as private photos or medical records, is stolen and leaked, it has the potential to create psychological harm such as considerable levels of stress, anxiety and embarrassment for individuals.

Additionally, one legacy of the recent surge in ransomware attacks targeting schools is the exposure of large amounts of safeguarding data and other sensitive pupil records.[248] Following a ransomware attack against Minneapolis schools in March 2023, threat actors leaked intimate and graphic reports about students that included descriptions of sexual assaults, domestic violence and mental health issues.[249] Many of the most sensitive files were posted on Twitter and Facebook, increasing the chance of families and pupils discovering them. Although none of the UK schools interviewed had pupil data stolen and leaked,

[248] Bajak, Hollingsworth and Fenn, 'Ransomware Criminals are Dumping Kids' Private Files Online After School Hacks'; Jonathan Greig, 'Microsoft Ties Vice Society Hackers to Additional Ransomware Strains', *The Record*, 25 October 2022, <https://therecord.media/microsoft-ties-vice-society-hackers-to-additional-ransomware-strains/>, accessed 5 December 2023.

[249] Bajak, Hollingsworth and Fenn, 'Ransomware Criminals are Dumping Kids' Private Files Online After School Hacks'; Collier, 'Hackers are Leaking Children's Data – And There's Little Parents Can Do'.

one leader at an academy trust emphasised that the attack on their schools caused fear among pupils, as they understood they were being targeted by criminals.[250] And while the Minneapolis schools example comes from a US context, similar events could also occur in the UK. Moreover, the fact that ransomware threat actors are finding it harder to monetise their operations means that there is a risk of them adopting the kind of extreme 'shaming' tactics like the ones used in the Minneapolis schools incident.[251]

It is worth emphasising that first-order harms to organisations and second-order harms to individuals can flow in both directions. For instance, a client's psychological distress may be sufficient for secondary victims to file legal action against organisations compromised by ransomware. In a recent case, patients launched a lawsuit against a cosmetic surgery provider after their pre- and post-operation photographs were leaked by ransomware operators.[252]

Second-order harms to organisations and individuals largely resemble the first-order harms. For organisations that experience indirect harm because a supplier has suffered a ransomware attack, this means they can still experience financial, reputational or physical/digital harm, but also often lack first-hand information about the evolving situation. Like the staff members who are direct victims of a ransomware attack, individuals outside the targeted organisation can also experience financial, psychological, or physical harm indirectly in the wake of the attack. Finally, although the risk to individuals due to ransomware operators' theft of personal data is currently low, this calculus could change in the future if cyber-criminals develop the intent and capability to exploit such data.

Third-Order Harms

This category of harms describes the cumulative effects of ransomware incidents on a state's economy, society and national security. Taken together, these harms emphasise the threat ransomware poses to states, as well as to organisations and individuals. It should be noted, however, that there are significant knowledge gaps about the impact of ransomware at a national level. This makes it challenging to assess the severity of the harm caused by ransomware to the UK and other countries, and creates the risk that governments will not prioritise and properly

[250] Author interview with Education 2, 16 December 2022.

[251] Author interview with Ransomware Specialist 3, 7 March 2023; Lily Hay Newman, 'Ransomware Attacks Have Entered a "Heinous" New Phase', *Wired*, 13 March 2023, <https://www.wired.com/story/ransomware-tactics-cancer-photos-student-records/>, accessed 5 December 2023.

[252] Graham Cluley, 'Women Sue Plastic Surgery After Hack Saw Their Indecent Photos Posted Online', BitDefender, 8 November 2023, <https://www.bitdefender.com.au/blog/hotforsecurity/women-sue-plastic-surgery-after-hack-saw-their-naked-photos-posted-online-2/>, accessed 5 December 2023.

resource responses to ransomware. This chapter draws on examples from both the UK and other countries.

Figure 6: Third-Order Harms to the Economy, National Security and Society

Economic	National Security	Societal
Supply chain disruptions	Reduced public safety	Disruption of essential services
Disruption of strategic companies	Disruption of defence supply chain	Loss of trust in essential services
Loss of economic output	Disruption of logistics	Opportunity costs for public sector
Loss of national productivity	Loss of trust in government/law enforcement	Loss of financial reserves for public sector organisations
	Strategic advantage for competitors (for example, Russia benefiting from actions of cyber-criminals)	Harms to individuals, disproportionately experienced by more vulnerable groups
		Normalisation of cybercrime

Source: Author generated.

Economic Harms

Ransomware has the potential to create considerable economic harm at a national level. However, there are significant challenges to be overcome when assessing the cost that ransomware exacts on the UK economy.

As highlighted elsewhere in this paper, ransomware operations generate costs and losses for victims, reduce productivity, lead to missed opportunities for growth, and disrupt supply chains, in turn spreading financial harms downstream to businesses of all kinds and scales. Disruptions of specific sectors or of individual companies that have significant market share of niche (but essential) products for global or national supply chains also have the potential to cause economic harm. One recent example of this was a ransomware attack against MKS, a US manufacturer that produces specialist parts and tools that are essential for companies making semiconductor chips.[253] The incident caused disruptions to the semiconductor supply chain – an essential component of modern digital infrastructure and the global economy.[254] As the challenges posed by Covid-19, geopolitical tensions and energy price rises have highlighted in recent years, disruptions to supply chains can have a wide range of negative effects that reach into all corners of a modern economy.[255]

[253] *Reuters*, 'Chip Equipment Maker MKS Instruments Says It is Investigating Ransomware Attack', 6 February 2023.

[254] Tim Bradshaw, 'Ransomware Attack on Chip Supplier Causes Delays for Semiconductor Groups', *Financial Times*, 28 February 2023.

[255] Institute for Government, 'Supply Chain Problems', 19 November 2021, <https://www.instituteforgovernment.org.uk/explainer/supply-chain-problems>, accessed 5 December 2023.

The sensitivity of modern globalised supply chains means that disruption to the operations of just one contributory logical element – for instance, imports at ports – have the potential to cause economic harm at scale.[256] An interviewee with first-hand experience of a protracted ransomware event in a developing country noted that its society had 'a total dependency on the customs system. Therefore, when this service disappeared, the imports and exports disappeared, the fruits were lost by the docks, they rotted. The technological products that we import, they were blocked. Everything was scarce in the country'.[257] Developed countries are also vulnerable to societal harms resulting from attacks on freight-related systems. A November 2023 incident against a shipping firm – responsible for 40% of Australian goods traffic – left shipping containers stuck at Australian ports.[258] This incident reportedly threatened the supply of Christmas goods, risked higher inflation, and raised the prospect of a future interest rate increase.[259]

However, while it is possible to describe the types of economic harms that ransomware causes a country, it is considerably more challenging to accurately calculate economic costs and losses. In order to assess the scale and scope of economic harm to the UK from ransomware, reliable costings for incidents are required, as well as aggregated quantitative data.[260]

Existing governmental, law enforcement and regulatory reporting mechanisms have several limitations in this regard. The UK Information Commissioner's Office has published data showing that since Q2 2019, there have been 1,940 ransomware incidents in the UK that required notification due to the risk to personal data.[261] However, data protection reporting is not focused on financial costs, and many attacks may not require ICO notification if the incident only encrypts servers that do not hold personal data.[262] Reporting of ransomware

[256] For examples, see Jacob Benjamin, 'OT Cybersecurity Breach Disrupts Operations at the Port of Nagoya, Japan', Dragos, 11 July 2023, <https://www.dragos.com/blog/ot-cybersecurity-breach-disrupts-operations-at-the-port-of-nagoya-japan/>, accessed 5 December 2023; Denys Reva, 'Cyber Attacks Expose the Vulnerability of South Africa's Ports', Institute for Security Studies, 29 July 2021, <https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports>, accessed 5 December 2023; Jana Winter, 'Exclusive: Ransomware Attacks on U.S. Supply Chain are Undermining National Security, CBP Bulletin Warns', *Yahoo News*, 21 March 2022, <https://uk.news.yahoo.com/exclusive-ransomware-attacks-on-us-supply-chain-are-undermining-national-security-customs-and-border-protection-bulletin-warns-191403260.html>, accessed 5 December 2023.

[257] Author interview with Foreign Government 1, 22 November 2022.

[258] Nick Bonyhady, 'DP World Checking Systems for Stolen Data, Software Threats After Hack', *Australian Financial Review*, 12 November 2023, <https://www.afr.com/technology/dp-world-checking-systems-for-stolen-data-software-threats-after-hack-20231110-p5ej43>, accessed 5 December 2023.

[259] Colin Kruger, David Swan and Shane Wright, 'Cyberattack Threatens to Spark Christmas Goods Shortage', *Sydney Morning Herald*, 12 November 2023, <https://www.smh.com.au/business/companies/cyberattack-threatens-to-spark-christmas-goods-shortage-20231112-p5ejcm.html>, accessed 5 December 2023.

[260] MacColl, Hüsch and Nurse, 'Beyond the Bottom Line: The Societal Impact of Ransomware'.

[261] ICO, 'Data Security Incident Trends', 1 November 2023, <https://ico.org.uk/action-weve-taken/data-security-incident-trends/>, accessed 5 December 2023.

[262] Martin, 'Ransomware Attacks Hit Record Level in UK, According to Neglected Official Data'.

incidents to law enforcement, meanwhile, is likely much lower. The UK's NCA, for instance, has estimated that less than 10% of victims report ransomware attacks to Action Fraud (the UK's national centre for reporting fraud and cybercrime).[263] Moreover, existing Action Fraud reporting mechanisms are not designed to capture the variety of costs and losses that ransomware imposes.

As noted in the section on first-order financial harms, surveys and other forms of research by cyber security vendors can shed some light on mean/median financial costs. Sophos's annual survey on ransomware includes figures on ransom payments, recovery costs and loss of business (although the 2023 version did not include these for the UK),[264] while IBM's annual Cost of a Data Breach report also includes the average cost of a ransomware attack.[265] Coveware, an incident response firm specialising in ransomware, also produces quarterly reports on mean/median ransom payments and incident length.[266] However, there is no standardised approach for calculating the costs and losses from ransomware, or their long-tail financial impact on other organisations, individuals or the economy. As a 2021 report from the US's Cybersecurity and Infrastructure Security Agency highlighted, there are considerable barriers to putting a value on the economic harm of ransomware and cyber incidents, be it for an individual victimised organisation or a country's economy as a whole.[267]

Harms to National Security

Ransomware is now widely considered to be a threat to national security in the US, Germany, Canada and the UK, among others.[268] Two primary harms to

[263] Cabinet Office, 'Written Evidence Submitted by His Majesty's Government', to the Joint Select Committee on the National Security Strategy, RAN0018, 30 January 2023, <https://committees.parliament.uk/writtenevidence/114408/pdf/>, accessed 8 July 2023.

[264] Sophos, 'The State of Ransomware 2023', <https://www.sophos.com/en-us/whitepaper/state-of-ransomware>, accessed 5 December 2023.

[265] IBM, 'Cost of a Data Breach Report 2023'.

[266] Coveware, 'Ransomware Quarterly Reports', <https://www.coveware.com/ransomware-quarterly-reports>, accessed 5 December 2023.

[267] CISA, 'Cost of a Cyber Incident: Systematic Review and Cross-Validation', 26 October 2020, <https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf>, accessed 5 December 2023.

[268] Sam Sabin, 'New White House Cyber Strategy Picks a Fight with Ransomware', *Axios,* 3 March 2023, <https://www.axios.com/2023/03/03/biden-cyber-strategy-ransomware>, accessed 5 December 2023; Danny Palmer, 'Ransomware is the Biggest Global Cyber Threat. And the Attacks are Still Evolving', *ZDNet*, 28 June 2022, <https://www.zdnet.com/article/ransomware-attacks-are-the-biggest-global-cyber-threat-and-still-evolving-warns-cybersecurity-chief/>, accessed 5 December 2023; United States Department of Justice et al., '2021 Trends Show Increased Globalized Threat of Ransomware', Joint Cybersecurity Advisory, AA22-040A, 9 February 2022, <https://www.ncsc.gov.uk/files/2021 Trends show increased threat of ransomware.pdf>, accessed 5 December 2023; HM Government, 'Security Minister CYBERUK Speech', 20 April 2023, <https://www.gov.uk/government/speeches/security-minister-cyberuk-speech>, accessed 5 December 2023; Federal Government of Germany, 'Integrated Security for Germany: National Security Strategy', 2023, <https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf>,

national security emanate from ransomware: the disruption of CNI and strategic sectors, with knock-on effects on economic prosperity and public safety; and the strategic advantage that ransomware can create for hostile states.

Ransomware operations targeting CNI in a number of different countries are now well publicised. The disruption of emergency services, energy infrastructure, telecommunications and healthcare has demonstrated the ability (or potential) of ransomware threat actors to cause harms to public safety. In some cases, ransomware operations have explicit implications for national defence. There are now several examples of cyber-criminals targeting defence and aerospace companies, disrupting defence supply chains,[269] or stealing sensitive data on intellectual property or military personnel.[270]

The growth of ransomware has also created strategic advantages for some states hostile to the UK and its allies. In the case of North Korea, ransomware operations by threat actors linked to the North Korean state are primarily financially motivated and aim to generate revenue for the regime.[271]

Meanwhile, the Russian-speaking ransomware ecosystem provides a number of advantages to the Russian state. Although the Russian state does not direct all cyber activity that emanates from within its borders, it provides a safe harbour, maintains close ties to some cyber-criminals or groups, and co-opts them or their capabilities for its own needs.[272] In 2019, the US Treasury highlighted the direct relationship between Evil Corp, a Russian cyber-criminal organisation responsible for a number of ransomware attacks, and Russia's Federal Security Service (FSB);[273] the same US Treasury advisory note suggested that Maksim Yakubets, one of the leaders of Evil Corp, was directly tasked by the FSB to conduct cyber espionage on its behalf.[274] In a similar vein, the organised cyber-

accessed 5 December 2023; *Reuters*, 'Cybercrime Set to Threaten Canada's Security, Prosperity – Spy Agency', 28 August 2023.

[269] Zack Whittaker, 'Defence Contractor CPI Knocked Offline by Ransomware Attack', *Tech Crunch*, 5 March 2020, <https://techcrunch.com/2020/03/05/cpi-ransomware-defense-contractor/>, accessed 5 December 2023.

[270] Renju Jose, 'Ransomware Hackers Hit Australian Defence Communications Platform', *Reuters*, 31 October 2022.

[271] NSA et al., 'StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities', 9 February 2023, <https://media.defense.gov/2023/Feb/09/2003159161/-1/-1/0/CSA_RANSOMWARE_ATTACKS_ON_CI_FUND_DPRK_ACTIVITIES.PDF>, accessed 5 December 2023.

[272] Justin Sherman, 'Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behaviour', Atlantic Council, 19 September 2022, <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/>, accessed 5 December 2023; Insikt Group, 'Cyber Threat Analysis: Russia', *Recorded Future*, 9 September 2021, <https://go.recordedfuture.com/hubfs/reports/cta-2021-0909.pdf>, accessed 5 December 2023.

[273] US Department of the Treasury, 'Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware', 5 December 2019, <https://home.treasury.gov/news/press-releases/sm845>, accessed 5 December 2023.

[274] *Ibid.*; Insikt Group, 'Cyber Threat Analysis'.

criminal group linked to the Conti ransomware operation was reportedly tasked by the FSB to collect intelligence on researchers at Bellingcat, an investigative non-profit organisation whose reporting has frequently embarrassed the Kremlin.[275]

The ransomware ecosystem also provides more indirect benefits to the Russian state. Russian intelligence units can benefit from using services, malware or tools developed by the criminal ecosystem to augment their own capabilities or provide plausible deniability for their own operations.[276] Moreover, while the vast majority of ransomware operations conducted by Russian cyber-criminals are financially, rather than ideologically, motivated, the fact that they harm the economic and societal resilience of the Kremlin's adversaries in North America and Europe is a useful by-product.

Societal Harm

As has been argued elsewhere, ransomware creates a range of societal harms.[277] Disruption of basic services, the diversion of resources from other priorities, and citizens' potential loss of trust in the state to protect them all illustrate the impact of ransomware on modern societies.[278] These types of harm are arguably less well understood or prioritised than those that more obviously affect economic prosperity and national security.

As highlighted earlier in this paper, the disruption of healthcare providers can degrade the quality of care that individual patients receive. Several participants stressed that the HSE incident in Ireland was one of the most impactful ransomware cases they had seen.[279] Harms to patient care can extend beyond the blast radius of an incident: one study in the US, for instance, showed that any hospitals physically adjacent to a hospital directly disrupted by a ransomware attack also experienced drops in their quality of patient care.[280] On a broader scale, ransomware operations targeting the healthcare sector can have cascading impacts that undermine the state's ability to provide or protect healthcare services. In national healthcare systems like the UK's NHS, single incidents can have systemic effects. In August 2022, for example, a ransomware operation against Advanced, a major NHS IT provider, caused disruption to NHS services

[275] Matt Burgess, 'Leaked Ransomware Docs Show Conti Helping Putin from the Shadows', *Wired*, 18 March 2022, <https://www.wired.co.uk/article/conti-ransomware-russia>, accessed 5 December 2023.

[276] Insikt Group, 'Cyber Threat Analysis'.

[277] MacColl, Hüsch and Nurse, 'Beyond the Bottom Line'.

[278] See Maria Bada and Jason Nurse, 'The Social and Psychological Impact of Cyberattacks', in Benson and McAlaney (eds), *Emerging Cyber Threats and Cognitive Vulnerabilities*, pp. 73–92.

[279] Author interview with DFIR 1, 5 December 2022; author interview with DFIR 3, 12 December 2022; incident response manager, RUSI workshop, 7 November 2022.

[280] Christian Dameff et al., 'Ransomware Attack Associated with Disruptions at Adjacent Emergency Departments in the US', *Jama Network*, 8 May 2022, <https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?resultClick=3>, accessed 5 December 2023.

that lasted for months, degrading the quality of patient care and increasing the workload of administrative and medical staff who were already under strain.[281]

The impact of ransomware on educational institutions also has societal implications. Although the UK government does not currently designate education as part of the country's CNI,[282] it plays an essential role in maintaining the development of a well-functioning society. Ransomware operations targeting the sector have grown in frequency, with one ransomware threat actor, Vice Society, seemingly deliberately targeting schools and universities. Although none of the interviewees from the education sector believed that the incidents involving their schools or universities caused lasting harm to students' education or outcomes,[283] such attacks create significant recovery costs for victims, and are often timed to coincide with the beginning of the school or academic year so as to maximise disruption.[284]

Beyond the immediate impact on the quality of life, wellbeing and development of citizens, ransomware operations against basic services also create significant opportunity costs and diversion of resources away from other priorities. Although these impacts also affect other organisations affected by ransomware, these types of harms, when inflicted on providers of public services, have societal implications. In the UK, ransomware attacks involving the NHS, state education or local authorities take place within a broader context of acute public spending constraints. At the time of writing, for instance, Hackney Council had spent £12.2 million on recovering from the attack in 2020, having previously experienced nearly a decade of some of the highest budget cuts in the country.[285] One interviewee from a UK local authority described how their council had been forced to use up most of its reserves to recover from an attack, diverting resources from other pressing issues.[286]

Finally, the prevalence of ransomware has the potential to undermine trust in the state. The workshops and interviews highlighted the low level of confidence that many victims and ransomware response providers have in the ability of the UK government (or law enforcement) to protect UK organisations or disrupt ransomware threat actors.[287] If citizens perceive the security of public services

[281] Joe Tidy and Katharine da Costa, 'Advanced Cyber-Attack: NHS Doctors' Paperwork Piles Up', *BBC News*, 30 August 2022.

[282] National Protective Security Authority, 'Critical National Infrastructure', 25 April 2023, <https://www.npsa.gov.uk/critical-national-infrastructure-0>, accessed 5 December 2023.

[283] Author interview with Education 2, 16 December 2022; author interview with Education 3, 10 January 2023.

[284] Greig, 'Microsoft Ties Vice Society Hackers to Additional Ransomware Strains'.

[285] Hackney Council, 'Council Calls for End to "Regressive Cuts" and Rethink of Funding Reform', 28 August 2019, <https://news.hackney.gov.uk/council-calls-for-end-of-regressive-cuts-and-rethink-of-funding-reform/>, accessed 5 December 2023.

[286] Author interview with Local Government 2, 1 March 2023.

[287] This will be explored in greater depth in a forthcoming paper for this project.

and data as being in doubt, they may lose confidence in the ability of law enforcement and government to protect them. One recent study of a ransomware attack against a hospital in Düsseldorf, Germany observed a sharp reduction in the local population's trust in the government and security agencies after the attack.[288] At present, though, there is little evidence that ransomware specifically has caused the UK public to lose trust in the NCSC or in law enforcement, although this could change if there were to be a significant attack against CNI.

While it is often challenging to directly link specific developments to a ransomware attack or to put a number on the financial cost of third-order societal harm caused by such attacks, the interview data has illustrated repeatedly that the harm caused by ransomware attacks has implications for wider society and national security, be it due to the interplay of cyber-criminals and state actors, or to the cumulative effects of ransomware harms on individuals, organisations, the economy and society at large.

[288] Miguel Alberto Gomez et al., 'Cyber Conflict and the Erosion of Trust', Council on Foreign Relations, 21 September 2022, <https://www.cfr.org/blog/cyber-conflict-and-erosion-trust>, accessed 5 December 2023.

III. Implications for Policy and Future Research

This paper has described the wide range of harms that ransomware attacks can cause and has provided examples of how victims – organisations as well as individuals – and countries experience these harms. In doing so, it starts to fill the knowledge gaps surrounding the ways ransomware causes harm to organisations, individuals and the UK as a whole. Deeper knowledge of these vectors of harm is critical to designing better responses to the ransomware threat and mitigating harm to victims. Several key findings from the research are important for pushing forward ransomware policy and future research. The next paper from this project will provide recommendations on how to mitigate some of the challenges laid out below.

1. **There is generally a low level of understanding of the long-term economic impact of ransomware attacks.**

At the time of writing, there are ongoing efforts within the UK government to calculate the economic impact of ransomware on the UK. Mobilising political will, prioritising intelligence and law enforcement resources, and building industry support for combating ransomware are to some extent all predicated on a clear costing of the harm being done to businesses and the UK economy. This paper has highlighted the wide range of costs, losses and downstream economic harms that must be included in any effort to calculate the economic impact of ransomware on the UK, but also the numerous challenges in doing so. For example, the costs of psychological harm caused to victims (impacting their productivity) and the long-term costs that might arise from additional staff turnover do not seem to be captured in interviewees' financial assessments, which focus predominantly on immediate costs – especially those that are recoverable via insurance. Including long-term and indirect costs, although methodologically challenging, would paint a more accurate picture of the true financial harm caused by ransomware.

In addition to these reporting challenges for governments and law enforcement, there is little evidence that victims or ransomware response services are collecting data on the full range of financial costs and losses from ransomware. This is partly due to the methodologically challenging nature of this task, but such data gathering is also hampered by the fact that many victims may not be resourced to assess the impact of incidents on their finances; moreover, victims sometimes have very little interest in dwelling on incidents. A number of interviewees highlighted that their organisation wanted to 'move on' in the aftermath of a ransomware attack, with little desire to measure or quantify long-term financial harms.

Just as victims are unlikely to have a comprehensive understanding of the financial harm inflicted, no stakeholder in the ransomware ecosystem possesses the long-term insights or general overview that would make possible an assessment of the wider economic harm. The other parties in the ecosystem (for instance, incident responders, insurers, legal counsel, law enforcement and regulators) only have limited insights into specific aspects of the financial harms and are therefore unable to collate all the information that is needed to make a comprehensive assessment of long-term financial harm. Likewise, it is unlikely that any other party would feel it was their responsibility to take on such a burdensome task. Consequently, it is unlikely that we will attain a comprehensive picture of long-term financial harm in the near future, meaning that the current figures probably underestimate the level of financial harm, since they are unlikely to have taken into account other forms of indirect additional costs or financial losses.

2. **Reputational harm is a major concern for organisations, but may be overestimated by victims in some contexts.**

Although the interview data confirmed that victims have a considerable fear of reputational harm, and that this often guides their response to incidents, the actual degree of reputational harm stemming specifically from data theft/exposure is not always as significant as imagined. Customers and clients can be forgiving, potentially indicating a wider societal acceptance that cyber security breaches cannot always be prevented. However, poor communication practices, both internally and externally, may have significant reputational consequences, as may the risk of data exfiltration. Reputational harm is also to some extent business- and sector-specific, and tightly interconnected with financial harm. Businesses that rely on continuous operations or that hold particularly sensitive information are more susceptible to reputational harm, which can lead directly to financial harm. Public sector organisations, on the other hand, are less exposed to reputational harm given that they often have a monopoly on the provision of basic services and that their funding is less dependent on reputational standing. While reputational harm should not be overlooked, the fact that such harm is often not as serious as some victims fear has important implications for organisations which believe that, in order to protect their reputation, they need to pay ransoms so that ransomware threat actors will delete stolen data.

3. **There is currently little evidence that exfiltrated data is systematically exploited for further criminal activities.**

Although there is wider concern about the potential for leaked data obtained in ransomware attacks to be exploited for fraud or other criminal activity, we have not found evidence that the ransomware ecosystem is exploiting stolen and leaked data in a systematic way. For the time being, exploiting stolen data is less profitable than extortion-based crime. While developments in cybercrime (particularly the skills and methods of large-scale data analysis) are likely to impact criminal practices in the future – with criminals potentially revisiting previously exploited data – our research indicates that such data is currently not being systematically exploited for criminal gains. This finding has implications for victims who believe they should pay ransoms to mitigate some of the risk from stolen and exfiltrated personal data.

4. **Psychological harm to staff and individuals is significantly overlooked, both in public discourse and in organisational responses to ransomware attacks.**

While the fear of reputational harm among victims is perhaps overstated in many instances, the opposite is true with regard to the psychological impacts of ransomware attacks, which are relatively neglected. Interviews highlighted that the psychological harm to staff is significantly overlooked, both in wider reporting and in organisational responses to ransomware attacks. Interviewees also repeatedly stressed that IT teams in particular suffer the psychological impacts of ransomware attacks. To reduce the harm caused by ransomware attacks, addressing the psychological impact on staff (and other individuals) needs to be at the centre of responses to a ransomware incident. This would involve not only raising awareness of potential psychological harm, but also ensuring that crisis management best practices focus on mitigating psychological harm.

5. **The second- and third-order harms from ransomware attacks disproportionately affect vulnerable groups.**

Ransomware attacks start by harming technology and organisations, but ultimately lead to harm to individuals. However, the effects on individuals are not felt equally. As noted above, within organisations, certain members of staff will likely experience more harm than others. Similarly, the external, downstream effects of ransomware may affect certain groups disproportionately. This is underlined by the impact that attacks on schools, hospitals, law firms that hold sensitive data, and local government services, have on vulnerable groups such as schoolchildren, healthcare patients and residents who rely on benefits or social care.

6. **Government responses to ransomware must focus more on highlighting and reducing societal harms, rather than focusing solely on economic harms.**

By targeting essential public services and other forms of CNI, ransomware harms the physical and mental health, development and prosperity of UK citizens. However, the enduring focus on the financial costs of ransomware risks making wider societal impacts seem abstract and unrelatable to policymakers and the public.[289] In the simplest terms, ransomware has the potential to ruin lives. More openness and clarity about the impact of ransomware on society may help to galvanise efforts, boost resources and increase the political will to find solutions. People – whether politicians or individual citizens – might be more likely to publicly categorise the cumulative effect of ransomware as a societal or national security risk if they knew that many cyber-criminals, some harboured by hostile states, regularly disrupt the services that are an essential part of modern society such as GP appointments, schools, and having rubbish bins collected by local councils.

This paper has underlined how impactful ransomware is upon individuals, organisations and wider society. Different forms of harm are felt by a wide range of individuals and groups, who are impacted directly or indirectly. To foster a better understanding of the necessity and nature of policy interventions, it is vital that policymakers understand the scale and breadth of ransomware harms. While ransomware crime is an intractable contemporary issue with no immediate solution,[290] action, where it is applied, should seek to increase resilience and alleviate harms. Greater attention urgently needs to be paid to the human impact of ransomware attacks, be it the psychological harm often overlooked in the wider discourse or the fact that vulnerable groups such as patients and benefits recipients are disproportionately impacted by ransomware harm.

[289] MacColl, Hüsch and Nurse, 'Beyond the Bottom Line'.
[290] Ransomware Taskforce, 'Combating Ransomware'.

Conclusion

Ransomware attacks remain a threat to individuals and organisations across the UK and indeed the globe. While the wider focus of reporting is often on the financial implications of ransomware attacks, this paper has set out a detailed analysis of different kinds of harm experienced directly or indirectly by ransomware victims and by society at large.

The interview data has suggested a framework including first-, second- and third-order harms to assist in distinguishing between those directly impacted by ransomware, those indirectly impacted, and the cumulative effect ransomware has on society at large. Within each order of harm, this paper identified several categories of harm, such as financial, psychological or reputational harm, and provided numerous examples of how such harm is experienced by victims.

Key findings based on this research underline that the psychological impact of ransomware attacks is significantly overlooked, and that currently no-one has a full understanding of the economic impact of ransomware attacks, such that the cost of the long-term and indirect financial harms is likely to be missing from current estimates of the economic harm caused by ransomware attacks. While the reputational harm stemming from a ransomware attack is a valid concern for some companies, especially those whose clients expect a higher level of privacy (such as customers of legal or financial services), the danger of reputational harm is often overestimated by victims. Similarly, the feared impact of exfiltrated data being used to cause further harm through financial fraud or other crime was not confirmed by interviewees. Instead, interview data showed that groups that are already vulnerable, such as benefits recipients or healthcare patients, are disproportionately impacted by ransomware harm. Finally, the paper found that government responses to ransomware attacks must focus on preventing societal harm.

The paper's detailed account of the ways in which ransomware attacks negatively impact individuals, organisations and society offers new insights into the actual harm caused by ransomware attacks. Although naturally limited, given that it reflects interview data and contemporary criminal activities that must be expected to evolve, the framework proposed in this paper will allow policymakers and practitioners – as well as those preparing for a potential cyber incident – to understand the ways in which victims are negatively impacted by ransomware attacks. This knowledge provides a critical baseline understanding for taking effective steps to mitigate such harm, both when responding or preparing for individual instances but also when designing policy interventions to tackle the ransomware threat. The framework further offers a valuable starting point for future analysis and data gathering, as findings from further research can be incorporated into the framework.

About the Authors

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 holds 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 holds a BA in War Studies from King's College London, where he was awarded the Sir Michael Howard Excellence Award in 2016 and 2018.

Pia Hüsch is a Research Analyst in 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, particularly under the principles of sovereignty and non-intervention. Previously, Pia has been a visiting researcher at McGill University and has worked at the Glasgow Centre for International Law and Security, as well as at the Brussels office of the German Marshall Fund of the United States. Pia's other research interests include the governance of cyberspace, election interference, cyber warfare and the relationship between law and technology, including cyber and AI. Pia holds 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. Prior to joining RUSI, he was a Lecturer in Security and Intelligence at the University of Kent. In this role, his research focused on the convergence of networked technologies and (inter)national governance. He convened a popular research-led module entitled 'Governance and War in Cyberspace', and supported the development of the university's Institute of Cyber Security for Society as an Organisational Lead. Previously, he was a Lecturer in International Relations at Nottingham Trent University. Gareth holds a PhD in International Relations (Security Studies) from Nottingham Trent University, completing an original thesis in 2018 on the spectre of cyber terrorism. He also holds an MA in International Security and a BA in International Relations and Modern History, both from the University of East Anglia.

James Sullivan is the Director of Cyber Research 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 fora such as the G7.

Jason RC 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 also holds the roles of 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. His 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*.

Sarah Turner holds 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 holds an MPA in Digital Technology and Public Policy from UCL's Department of Science, Technology, Engineering and Public Policy (STEaPP). 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 PhD student in Computer Science at the University of Kent and a member of the Institute of Cyber Security for Society. Blending 25 years of experience in both academia and the IT sector across the UK, Oman and India, she works on the security dynamics of a connected home environment. Her research interest includes cyber security and privacy perspectives of users in multi-user homes with multiple devices, insider threats in multi-user homes, 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 holds a degree in Analytical Economics from Utkal University and a BSc in Computer Science from the Open University.