Occasional Paper

Cyber Insurance and the Ransomware Challenge

Jamie MacColl, James Sullivan, Jason R C Nurse, Sarah Turner, Gareth Mott, Edward Cartwright and Anna Cartwright

Occasional Paper

192 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 192 years.

Published in 2023 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, July 2023. ISSN 2397-0286 (Online).

Cover Image: Concept art of a padlock on a digital network. Generated with AI. *Courtesy of Torsten / Adobe Stock.*

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 and the Research Institute for Sociotechnical Cyber Security for providing funding for this paper and their support throughout the research process.

A great deal of thanks must go to the team that helped to guide and shape this paper. Hugh Oberlander, Dina Mansour-Ille and the Publications Team all provided valuable support and editing. The authors would also like to thank Joseph Jarnecki, who contributed to the literature review that informed Chapter I of this report.

Thanks also go to the peer reviewers, including Dr Lucy Fraser of the ABI, as well as the various individuals from government and the insurance industry who provided insightful feedback on different stages of the report and the recommendations.

A final thank you goes to the participants in this research, to all those who very kindly gave up their time to participate in interviews and workshops. Every single interview contributed greatly to the authors' thinking and findings.

Executive Summary

The cyber insurance industry has been heavily criticised for providing coverage for ransom payments. A frequent accusation, which has become close to perceived wisdom in policymaking and cyber security discussions on ransomware, is that cyber insurance has incentivised victims to pay a ransom following a cyber incident, rather than seek alternative remediation options. Over a 12-month research project, researchers from RUSI, the University of Kent, De Montfort University and Oxford Brookes University conducted a series of expert interviews and workshops to explore the relationship between cyber insurance and ransomware in depth. This paper argues that there is, in fact, no compelling evidence that victims with cyber insurance are much more likely to pay ransoms than those without.

Ransomware remains one of the most persistent cyber threats facing the UK. Despite a range of government, law enforcement and even military cyber unit initiatives, ransomware remains lucrative for criminals. During this research, we identified three main drivers that ensure its continued success:

1. A profitable business model that continues to find innovative ways to extort victims.
2. Challenges around securing organisations of all sizes.
3. The low costs and risks for cybercriminals involved in the ransomware ecosystem, both in terms of the barriers to entry and the prospect of punishment.

Despite this perfect storm of factors, the cyber insurance industry has been singled out for criticism with the claim that it is funding organised cybercrime by covering ransom payments. In reality, cyber insurance's influence on victim decision-making is considerably more nuanced than the public debate has captured so far. While there is evidence that cyber insurance policies exfiltrated during attacks are used as leverage in negotiations and to set higher ransom demands, the conclusion that ransomware operators are deliberately targeting organisations with insurance has been overstated.

However, the insurance industry could do much more to instil discipline in both insureds and the ransomware response ecosystem in relation to ransom payments to reduce cybercriminals' profits. Insurers' role as convenors of incident response services gives them considerable power to reward firms that drive best practices and only guide victims towards payment as a last resort. But the lack of clearly defined negotiation protocols and the challenges around learning from incidents make it difficult to develop a sense of collective responsibility and shared best

practices around ransomware response. This has not been helped by the UK government's black-and-white position on ransom payments, which has created a vacuum of assurance and advice on best practices for ransom negotiations and payments.

This paper does not advocate for an outright ban on ransom payments or for stopping insurers from providing coverage for them. Instead, it makes the case for interventions that would improve market-wide ransom discipline so that fewer victims pay ransoms, or pay lower demands. Ultimately, this involves creating more pathways for victims that do not result in ransom payments.

Beyond ransom payments, cyber insurance has a growing role in raising cyber security standards, which could make it more difficult to successfully compromise victims and increase costs for ransomware operators. Successive years of losses from ransomware have led to more stringent security requirements and risk selection by underwriters. Although the overall effect of this on the frequency and severity of ransomware attacks remains to be seen, by linking improvements in security practices to coverage, cyber insurance is currently one of the few market-based levers for incentivising organisations to implement security controls and resilience measures. However, continued challenges around collecting and assessing reliable cyber risk and forensic claims data continue to place limits on the market's effectiveness as a mechanism for reducing ransomware risk. This, along with cyber insurance's low market penetration, makes clear that cyber insurance should not be treated as a substitute for the legislation and regulation required to improve minimum cyber security standards and resilience. Insurers are also commercial entities that primarily exist to help organisations transfer risk, rather than to improve national security and societal cyber resilience.

The cyber insurance industry could be a valuable partner for the UK government through increased ransomware attack and payment reporting, sharing aggregated claims data, and distributing National Cyber Security Centre (NCSC) guidance and intelligence to organisations. However, the government has not made a compelling enough case to insurers and insureds about the benefits of doing so. Instead, it has relied on appealing to their general sense of altruism. While insurers will benefit if governments are able to generate more accurate and actionable data on ransomware, albeit indirectly, this needs to be sold to the industry in a more convincing way.

Some principles and recommendations for both the insurance industry and the UK government are listed below. These are not designed to solve all the challenges of the cyber insurance market, nor do they present wide-ranging solutions to the ransomware challenge. Instead, they focus on where the cyber insurance industry can have the most impact on key ransomware drivers. This reflects the

fact that disrupting the ransomware economy involves applying pressure from different angles in a whole-of-society approach. The recommendations also start from the position that the UK government's light-touch approach is unsustainable and requires more intervention in private markets that are involved in ransomware prevention and response. While they are specifically aimed at UK policymakers, regulators and insurers, they may be applicable to other national contexts.

Recommendations

Recommendation 1: To increase oversight of ransomware response, insurers should use policy language to require that insureds and incident response firms provide written evidence of negotiation strategies and outcomes.

Recommendation 2: To develop and drive ransomware response best practices across the market, insurers should select specialist ransomware response firms for panels that meet a set of pre-defined minimum requirements. These should include:

- A proven track record of both regularly achieving outcomes that do not result in ransom payments, and of operational relationships with law enforcement and cyber security agencies.
- Conducting sanctions risk assessments.
- Compliance with anti-money laundering laws and FATF (Financial Action Task Force) standards.
- Ensuring payment firms that make payments on behalf of UK victims are registered with relevant financial authorities in the UK.

Recommendation 3: The UK government should commission a study to improve its understanding of specialist ransomware response firms. This should aim to identify common best practices and key market players, and create a framework for benchmarking the quality of their services and products. These findings can be distributed to trusted partners in the insurance industry. To drive best practices in ransomware response and create more oversight of the incident response ecosystem, the NCSC, National Crime Agency (NCA) and international partners should also explore the feasibility and potential implications of creating a dedicated assurance scheme for firms that provide specialist ransomware services such as decryption, recovery, negotiations and payments.

Recommendation 4: To increase reporting of ransom payments, the UK government and international partners should explore creating a dedicated licensing regime for firms that facilitate cryptocurrency payments on behalf of ransomware victims. In the short-term, the UK government should follow the

example set by the US government and also ensure that ransomware response firms that facilitate payments are registered as money service businesses in the UK and therefore subject to national financial crime reporting requirements.

Recommendation 5: To reach a market-wide consensus on what constitutes a reasonable last resort before a ransom payment is made, insurers should agree on a set of minimum conditions and obligations in ransomware coverage to ensure alternatives are explored first. These should include sanctions due diligence, a requirement to notify law enforcement and written evidence that all options have been exhausted.

Recommendation 6: To increase ransomware reporting and ensure victims are able to access any relevant law enforcement and NCSC support, insurers should specify that any ransomware coverage must contain a requirement for policyholders to notify Action Fraud (the UK's national centre for reporting fraud and cybercrime) and the NCSC before a ransom is paid. If there is no progress on this recommendation without intervention, then regulators should intervene to compel insurers to include this obligation in coverage. However, this recommendation also depends on the implementation of long-promised but delayed reforms to Action Fraud. These should include creating a dedicated category for reporting ransomware. Law enforcement and the NCSC must also provide assurances to insurers that they have the capabilities to support victims during incidents and that reporting leads to actual outcomes against ransomware actors, such as cryptocurrency seizures, arrests or offensive cyber operations.

Recommendation 7: The NCSC and a UK insurer should trial integrating the NCSC's Early Warning service into their ongoing assessments of policyholders. This would enable the insurer to distribute intelligence from Early Warning at scale and notify policyholders of potential ransomware attacks. The NCSC should also explore whether Early Warning will need to be expanded and adapted to meet the requirements of insurers and policyholders.

Recommendation 8: To deepen operational collaboration with the insurance industry, the NCSC should seek to recruit secondees from the cyber insurance industry into the Industry 100 cyber security secondment scheme. This should include identifying specific tasks and roles for underwriters, claims managers and incident response professionals working for UK insurers.

Recommendation 9: To increase reporting of ransom payments, the Home Office and NCA should ensure that existing financial crime reporting mechanisms – specifically, suspicious activity reports (SARs) – are fit for reporting ransom payments or money laundering linked to ransomware. Concurrently, the UK government should also identify ways to encourage cyber insurers to report ransom payments as SARs or through more informal channels.

Introduction

Ransomware threatens the UK's national security and economic resilience. In February 2022, the UK's National Cyber Security Centre (NCSC) stated that it 'recognises ransomware as the biggest cyber threat facing the United Kingdom'.[1] The impacts on businesses, charities and critical national infrastructure have mounted, in terms of both financial costs and downtime of essential services. The ransomware ecosystem has professionalised and specialised over recent years, supporting a surge in attack severity.[2] A permissive law enforcement environment for Russian cybercriminals, the difficulty and cost of securing the IT infrastructure of businesses and public sector organisations, and an effective business model have all enabled this ecosystem to thrive.[3] Ransomware is now a global criminal enterprise that has paid significant dividends to those who participate. The growth of ransom payments and large profit margins have enabled ransomware operators to reinvest revenues, expand their capabilities and stay ahead of cyber defences and law enforcement.[4]

Ransomware's rise has also created considerable challenges for the cyber insurance market. Consecutive years of losses from ransomware have now created a very different, so-called 'hard' cyber insurance market, with rising premiums, more restricted and conditional coverage, and tougher cyber security requirements.[5] The market is expected to fluctuate further as insurers seek ways to generate profits in 2023.

Cyber insurance was developed long before ransomware became a significant problem. Organisations purchasing policies originally sought to cover the costs of privacy breaches and other types of liability, rather than the kind of operational risk that ransomware poses.[6] As profits grew, new entrants who were unprepared or unable to grapple with the complexities of cyber risk joined the market. Fierce competition to grow market share and profits created a race to the bottom, with

1. US Department of Justice et al., '2021 Trends Show Increased Globalized Threat of Ransomware', Joint Cybersecurity Advisory, AA22-040A, 9 February 2022.
2. David S Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic', *European Law Enforcement Research Bulletin* (No. 22, 2022), pp. 45–60.
3. James Sullivan and James Muir, 'Ransomware: A Perfect Storm', RUSI Emerging Insights, March 2021; Ransomware Task Force, 'Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force', Institute for Security and Technology, April 2021.
4. Coveware, 'Ransomware Attackers Down Shift to "Mid-Game" Hunting in Q3 2021', 21 October 2021, <https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts>, accessed 30 November 2022.
5. Carolyn Cohn, 'Insurers Run From Ransomware Cover as Losses Mount', *Reuters*, 19 November 2021.
6. Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks* (Cambridge, MA: MIT Press, 2022).

falling prices and broader coverage. These conditions also meant that insurers could not incentivise or compel policyholders to improve their cyber risk posture, even when they wanted to.[7] These factors created a perfect storm for many insurers, as ransomware increased in severity.

At the same time, some policymakers, researchers and cyber security practitioners have suggested that cyber insurance has driven the growth in ransomware. Critics of the industry claim that insurers have been too ready to reimburse ransom payments as doing so is perceived to be cheaper than rebuilding IT systems or covering the potential liability related to stolen data, causing ransom inflation and incentivising further attacks. An additional charge laid against cyber insurance is that ransomware operators specifically target organisations with policies as a way to extract higher payments and increase the victim's likelihood to pay.

Ransomware may present opportunities as well as challenges for the development of cyber insurance as a form of cybercrime governance. As highlighted in a previous RUSI Occasional Paper and elsewhere, there is longstanding interest in the potential role that cyber insurance could play in mitigating the impact of cybercrime by improving policyholders' cyber security and resilience.[8] Although that research highlighted plenty of unfulfilled potential in this regard, the current hard market and ransomware's political salience provide an opportunity for reassessment. Moreover, recent research has illustrated a nascent framework for establishing a form of cyber-insurance-based governance to mitigate some of the costs and impact of ransomware by drawing on lessons from the kidnap-for-ransom insurance market.[9]

7. Jamie MacColl, Jason R C Nurse and James Sullivan, 'Cyber Insurance and the Cyber Security Challenge', *RUSI Occasional Papers* (June 2021); Daniel Woods, 'The Evolutionary Promise of Cyber Insurance', The FinReg Blog, 1 February 2022, <https://sites.duke.edu/thefinregblog/2022/02/01/the-evolutionary-promise-of-cyber-insurance%EF%BF%BC/>, accessed 10 October 2022.
8. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'; Daniel W Woods and Tyler Moore, 'Does Insurance have a Future in Governing Cybersecurity?', *Security and Privacy* (Vol. 18, No. 1, 2020); Erin Kenneally, 'Ransomware: A Darwinian Opportunity for Cyber Insurance', *Connecticut Insurance Law Journal Fall Symposium Edition* (Vol. 28, No. 1, 2021); Jason R C Nurse et al., 'The Data That Drives Cyber Insurance: A Study into the Underwriting and Claims Processes', paper presented at IEEE Cyber Science 2020, International Conference on Cyber Situational Awareness (online), June 2020; Daniel Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms', *Journal of Internet Services and Applications* (Vol. 8, No. 8, 2017).
9. Anja Shortland, Tom Keatinge and Jamie MacColl, 'Insurance as Crime Governance: Comparing Kidnap for Ransom and Ransomware', *RUSI Whitehall Report*, 2-23 (April 2023); Tom Baker and Anja Shortland, 'The Government Behind Insurance Governance: Lessons for Ransomware', *Regulation and Governance*, 22 October 2022.

In light of this, this paper attempts to answer two research questions:

1. To what extent is cyber insurance enabling the ransomware ecosystem by covering payments?
2. Can cyber insurance help disrupt the ransomware ecosystem?

The paper's recommendations derive from a series of interviews and a workshop. They mainly suggest ways in which the UK can better use cyber insurance to disrupt the ransomware ecosystem. Their formation involved sustained engagement with experts in cyber insurance underwriting, incident response and ransomware negotiations.

Structure

The paper is divided into five chapters. Chapter I outlines ransomware drivers and enablers, and what kind of coverage cyber insurance provides for ransomware incidents. Chapter II examines the debates and evidence around cyber insurance's potential role in fuelling or mitigating the ransomware business model. Chapter III explores how the cyber insurance industry can contribute to broader efforts to combat ransomware by raising cyber security standards across organisations. Chapter IV assesses how cyber insurance could support government and law enforcement activity against cybercriminals. The paper concludes with a set of targeted recommendations for the UK government and the insurance industry.

Methodology

This paper forms part of a 12-month research project conducted by RUSI, the University of Kent, De Montfort University and Oxford Brookes University entitled 'Ransomware and Cyber Insurance'. It is funded by the NCSC, in collaboration with the Research Institute in Sociotechnical Cyber Security. The project aims to explore the relationship between ransomware and cyber insurance.

The data collection and analysis for this paper consisted of a literature review, semi-structured interviews and a workshop.

- **Literature review**: The project began with a literature review of publicly available sources to map the current stakeholder landscape and pertinent debates. Sources included government and policy documents, academic articles, media reporting, and surveys and reports from the insurance and cyber security industries.
- **Semi-structured interviews**: The primary dataset for this paper is based on 65 semi-structured interviews with subject-matter experts from across the

insurance and cyber security industries, law firms, UK government and law enforcement agencies. It also includes interviews with individuals responsible for purchasing cyber insurance within industry. Interviewees were chosen based on their expertise and experience, using a non-probabilistic (selective) sampling method. Other participants were then identified through snowball sampling. The interviews were conducted in person and online between September 2021 and February 2022. They were anonymised to allow individuals to speak openly about potentially sensitive issues. The research team then analysed the interview transcripts using a thematic analysis approach,[10] which involved generating codes that reoccurred in interviews and identifying themes that provided insight into the research questions. An anonymised coding system shown in Table 1 is used to refer to interview data in the footnotes.

- **Workshop**: The research team conducted an online workshop with key stakeholders from UK government, the insurance and cyber security industries, law enforcement and businesses in February 2022. The workshop had 49 participants, including a mix of interviewees and new participants using the contacts established at the interviews. It was used to validate and reassess themes identified in the literature review and interviews.

10. Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology', *Qualitative Research in Psychology* (Vol. 3, No. 2, 2006), pp. 77–101.

Table 1: Breakdown of Interviewees

Category	Subcategory/Role	Count
Insurance industry	Cyber insurance underwriter	10
	Cyber insurance broker	5
	Cyber insurance claims	3
	Cyber insurance executive	3
	Insurance industry association	3
	Cyber risk management services	2
	Cyber reinsurance executive	1
	Cyber reinsurance underwriter	1
	Cyber risk analytics	2
Cyber security	Digital forensics and incident response (DFIR)	9
	Cyber threat intelligence (CTI)	3
	Cyber security consultant	3
	Public policy	1
	Ransomware negotiations and recovery[11]	1
	Cyber security recruitment	1
Purchasing organisations	Technology	2
	Local government	2
	Financial services	1
	Transport	1
	Defence	1
UK government	Cyber policy	3
	Incident management	1
Professional services	Breach counsel	2
	Insurance lawyer	1
Law enforcement	International law enforcement agency	1
	UK law enforcement agency	1
Academia	Academic	1
Total		**65**

Source: Author generated.

Note: The report references interviewees with the subcategory/role and a number, e.g. 'Cyber insurance underwriter 4' to maintain anonymity while also allowing the reader to differentiate between interviewees from the same stakeholder categories.

11. Note that other interviewees from DFIR firms provide some of the services that specialist ransomware firms provide, such as ransomware negotiations.

Key Definitions and Terms

Cyber security and cyber insurance are replete with acronyms and jargon. While this paper is intended to be accessible to all readers, some less familiar vocabulary will inevitably be used. For instance, 'insured' refers to the buyer and beneficiary of insurance provided by an insurer. Insurance is often referred to as 'coverage', and a market in which demand for insurance outstrips supply is often termed 'hard', meaning the insurer has the upper hand in setting prices or conditions for cover. The paper uses a broad definition of ransomware that includes extortion related to the exfiltration and encryption of data (see Chapter I). When referring to criminals involved in the ransomware economy, the paper makes a distinction between 'ransomware operators', who develop and maintain the infrastructure and tools behind ransomware operations, and 'ransomware affiliates', who are responsible for delivering the ransomware payload and/or exfiltrating data in exchange for a cut of profits.[12]

Scope and Limitations

There are three main limitations to the generalisability of this paper's findings. First, the insurance market has experienced profound changes over the past several years. As most interviews were conducted in 2021 and 2022, the latest round of insurance and reinsurance renewals in January 2023 may have impacted some of the market dynamics identified here. Second, findings may only be representative of UK and US contexts, but it should be noted that many of the participants (especially cyber insurers in the Lloyd's market) underwrite insurance internationally. Finally, despite best efforts to minimise sampling bias, some sectors are more represented than others.

12. A longer list of terminologies can be found in Annex 1.

I. The Rise of Ransomware and its Impact on the Cyber Insurance Market

Understanding the drivers and enablers of ransomware's success is essential for assessing how cyber insurance could disrupt this ecosystem. This chapter also provides an overview of ransomware insurance coverage and the current state of the market.

Ransomware has emerged as a highly lucrative criminal enterprise over the past decade. Since 2019, the ecosystem has become increasingly professionalised, with operators finding new ways to increase leverage and extort victims. A range of technological, political, and economic drivers and enablers have facilitated its profitability. The fortunes and profitability of the cyber insurance market have also become increasingly intertwined with ransomware's growth. Many cyber insurers were unprepared for rising claims and losses from ransomware attacks following a race to the bottom in underwriting standards and pricing. This has helped to create a so-called 'hard' insurance market for cyber risk.

The Rise of Ransomware

What is Ransomware?

Ransomware has historically been defined as a form of malware that disrupts a user's access to their computer system. However, in recent years 'ransomware' has become a catch-all term for different types of cyber extortion – including data theft. Indeed, some 'ransomware' attacks now only steal data, rather than encrypt it. As such, this paper follows the Ransomware Task Force's broader definition of ransomware as activity where threat actors compromise computer systems, demanding a ransom for the restoration or non-exposure of encrypted and/or stolen data and systems.[13]

13. Ransomware Task Force, 'Combating Ransomware', p. 5.

Evolution From 'Spray and Pray' to a Professionalised Economy

Prior to the early 2010s, the first generation of ransomware was largely non-viable as a profitable and scalable cybercrime.[14] This changed with the integration of strong and stable encryption, using tools such as RSA public-key cryptography, and the greater anonymity that cryptocurrency provides.[15] Early ransomware operations relied on scale, conducting so-called 'spray and pray' campaigns against a large number of individual users.[16] CryptoLocker, the most successful ransomware strain of this period, infected an estimated 234,000 computers and extorted $30 million over a two-month period in the winter of 2013.[17] Yet, for the most part, ransomware operations were not nearly as profitable as future iterations. Attacks had low yields, with uniformly priced ransoms for all victims.

In 2016, there were early signs that ransomware was beginning to evolve into something different.[18] The collapse of the profitability of credit-card-based fraud in the mid-2010s brought more professional and organised cybercriminals into the ransomware business.[19] Ransomware operators also began to move away from the 'spray and pray' model and targeted organisations instead of individual users. By gaining access to administrator accounts through poorly secured remote access services, cybercriminals could escalate privileges and deploy their payload to thousands of computers within a single organisation.[20] Although these types of ransomware operations have been described as 'targeted', they still relied on opportunism to gain access to victims. For instance, ransomware operators in this period (and still today) often relied on mass-scanning for poorly secured Remote Desktop Protocol (RDP) ports, or purchased access to victims from cybercriminal marketplaces that specialised in compromising RDP.[21]

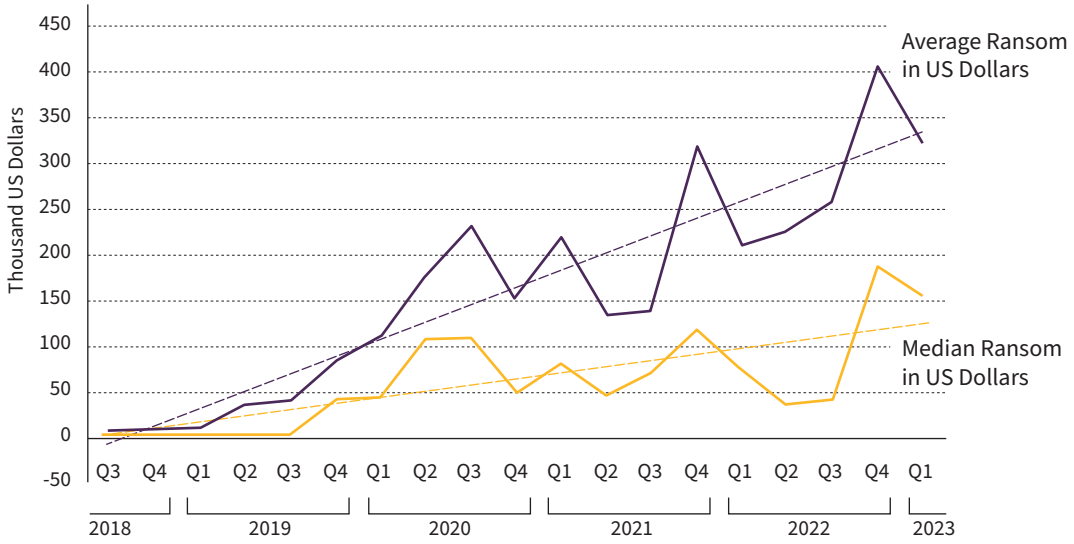
14. This section largely draws on existing research, particularly: Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic'; John Sakellariadis, 'Behind the Rise of Ransomware', Issue Brief, Atlantic Council, 2 August 2022.
15. J Hernandez-Castro, A Cartwright and E Cartwright, 'An Economic Analysis of Ransomware and Its Welfare Consequences', *Royal Society Open Science* (4 March 2020), pp. 1–14.
16. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic', p. 48.
17. Gail-Joon Ahn et al., 'Ransomware and Cryptocurrency: Partners in Crime', in Thomas J Holt (ed.), *Cybercrime Through an Interdisciplinary Lens* (Abingdon: Routledge, 2019), pp. 105–24.
18. Wall, 'The Transnational Cybercrime Extortion Landscape and the Pandemic'; Sakellariadis, 'Behind the Rise of Ransomware'; see also Trend Micro, 'A Deep Dive Into the Evolution of Ransomware: Part 1', 21 February 2023, <https://www.trendmicro.com/en_ie/research/23/b/ransomware-evolution-part-1.html>, accessed 9 July 2023.
19. Sakellariadis, 'Behind the Rise of Ransomware'.
20. *Ibid*.
21. See Coveware, 'Don't Become a Ransomware Target – Secure Your RDP Access Responsibly', 8 January 2019, <https://www.coveware.com/blog/dont-become-a-ransomware-target-secure-rdp>, accessed 9 July 2023. Danny Palmer, 'Dark Web Vendors are Selling Remote Access to Corporate PCs for as Little as $3', *ZDNET*, 24 October 2017, <https://www.zdnet.com/article/dark-web-vendors-are-selling-remote-access-to-corporate-pcs-for-as-little-as-3/>, accessed 7 July 2022.

Since 2018, ransomware has become increasingly professionalised and organised, with cybercriminals adopting business and tactical innovations that allow them to extort higher payments at greater scale. The development of the ransomware-as-a-service (RaaS) model has enabled the specialisation of roles within groups, allowing ransomware developers to recruit 'affiliates' who conduct operations on behalf of the ransomware developers for a cut of the profit.[22] The core impetus for the emergence of a range of 'collaborative' or 'service-oriented' ransomware models is that these offer tantalising scope for ransomware operators to increase the scale and volume of their attacks. RaaS operations integrate other actors from within the cybercrime ecosystem, particularly botnet operators and other cybercriminals who specialise in gaining access to victim networks.[23]

Another tactical modification in recent years relates to victim selection. Some ransomware operators shifted their focus to larger businesses in 2019. So-called 'big game hunting' ransomware operations caused average ransom payments to grow significantly,[24] as seen in Figure 1. By 2021, ransomware operators were netting ransom payments as high as $40 million from a single attack.[25] To maximise revenue, ransomware operators also put more emphasis on targeting critical services and organisations that rely on constant delivery of operations to exert maximum leverage. During the Covid-19 pandemic, for instance, some ransomware groups were relentless in their targeting of healthcare organisations.[26]

22. Intel471, 'Ransomware-as-a-service: The Pandemic Within a Pandemic', Intel471 Blog, 16 November 2020, <https://intel471.com/blog/ransomware-as-a-service-2020-ryuk-maze-revil-egregor-doppelpaymer>, accessed 9 July 2023; Microsoft Threat Intelligence, 'Ransomware as a Service: Understanding the Cybercrime 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 9 July 2023.
23. Victoria Kivilevich, 'Ransomware Gangs are Starting to Look Like Ocean's 11', KELA, 8 July 2021, <https://www.kelacyber.com/ransomware-gangs-are-starting-to-look-like-oceans-11/>, accessed 9 July 2023; Brian Krebs, 'Conti Ransomware Group Diaries, Part II: The Office', KrebsonSecurity, 2 March 2022, <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/>, accessed 9 July 2023.
24. Sean Gallagher, 'FBI Warns of Major Ransomware Attacks as Criminals Go Big-Game Hunting', *Ars Technica*, 7 July 2019, <https://arstechnica.com/information-technology/2019/10/fbi-warns-of-major-ransomware-attacks-as-criminals-go-big-game-hunting/>, accessed 9 July 2023; Coveware, 'Ransomware Costs Double in Q4 as Ryuk, Sodinokibi Proliferate', 23 January 2020, <https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate>, accessed 20 July 2023.
25. Kartikay Mehrotra and William Turton, 'CNA Financial Paid $40 Million in Ransom After March Cyberattack', *Bloomberg*, 20 May 2021.
26. 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 17 May 2022.

Figure 1: The Value of Ransomware Payments, Q3 2018–Q1 2023



Source: Coveware, 'Ransomware Quarterly Reports', <https://www.coveware.com/ransomware-quarterly-reports>, accessed 20 June 2023.

Innovations in extortion tactics have also proliferated since late 2019. Pioneering ransomware operators adopted so-called 'double extortion' tactics, exfiltrating victim data which they then threatened to leak unless the ransom was paid. The criminals behind Maze ransomware pioneered this approach in 2019, also launching a name-and-shame leak site where they could release victim data to increase their leverage.[27] By early 2020, 70% of ransomware operations tracked by Coveware, a specialist ransomware response firm, utilised double extortion.[28] Coercion tactics have continued to evolve, and include distributed denial of service attacks, cold calling employees and clients, leaking to journalists, contacting business partners and clients, harassing employees, and selectively auctioning high-profile data.[29] In some cases, double extortion has escalated to triple extortion, as ransomware operators threaten the clients or business partners of the original victims with data leaks unless a ransom is paid.[30]

27. Catalin Cimpanu, 'Here's a List of All the Ransomware Gangs Who Will Steal and Leak Your Data If You Don't Pay', *ZDNET*, 21 April 2020, <https://www.zdnet.com/article/heres-a-list-of-all-the-ransomware-gangs-who-will-steal-and-leak-your-data-if-you-dont-pay/>, accessed 2 March 2023.
28. Coveware, 'Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands', 1 February 2021, <https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020>, accessed 10 October 2022.
29. ENISA, 'ENISA Threat Landscape 2021: April 2020 to Mid–July 2021', October 2021, pp. 25–26.
30. US Department of Justice et al., '2021 Trends Show Increased Globalized Threat of Ransomware', p. 3.

Ransomware in 2023

The state of the ransomware ecosystem at the time of writing is less clear. While attacks continue and ransomware operators still bring in high revenues, there are signs that the traditional RaaS affiliate model may be in flux. Prominent attacks against critical national infrastructure in 2021, including Colonial Pipeline, have generated a heavy response from US authorities and some allies, including sanctions, intensified law enforcement activity and even offensive cyber operations against ransomware operators' infrastructure. This has also made ransomware developers wary of delegating independence to affiliates who are less discerning in their choice of victims. The war in Ukraine may have also exposed divisions in the ransomware ecosystem between Ukrainian and Russian cybercriminals.[31]

The current ecosystem is likely to be more fluid, with ransomware developers rebranding their products more regularly to evade sanctions and law enforcement operations, and affiliates potentially being less loyal to particular RaaS operations due to rising levels of distrust.[32] But it is too early to say that the ransomware challenge is improving. Although there have been some encouraging signs that the profits of ransomware criminals may have declined in 2022,[33] data from 2023 so far suggests that ransomware will remain a risk for the foreseeable future.[34]

The Drivers and Enablers of Ransomware

To understand how cyber insurance might play a role in combating the ransomware threat, it is worth briefly summarising the drivers and enablers of the ransomware challenge to explain how we have reached the present situation.

31. Aaron Schaffer, 'Ransomware Hackers Have a New Worst Enemy: Themselves', *Washington Post*, 12 October 2022.
32. *Ibid.*; John Fokker, 'Dismantling a Prolific Cybercriminal Empire: REvil Arrests and Reemergence', Trellix, 29 September 2022, <https://www.trellix.com/en-us/about/newsroom/stories/research/dismantling-a-prolific-cybercriminal-empire.html>, accessed 2 March 2022.
33. Chainalysis, 'Ransomware Revenue Down as More Victims Refuse to Pay', 19 January 2023, <https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/>, accessed 20 June 2023.
34. Sam Sabin, 'Ransomware Is a Forever Problem Now', 29 April 2023, Axios, <https://www.axios.com/2023/04/28/ransomware-attack-cybersecurity-rsa-conference>, accessed 20 June 2023; Tim Starks, 'Think Ransomware Gangs Won't Thrive This Year? Think Again, Experts Say', *Washington Post*, 30 March 2023.

Table 2: The Drivers and Enablers of Ransomware

Drivers	Enablers
A highly profitable and efficient business model	**The growth of ransom payments**. Ransoms have become the most profitable source of income for many cybercriminals. As such, ransomware groups have continued to find effective ways to coerce and compel victims to pay ransoms. Although paying them is not a silver bullet, for many victims it is – or is perceived to be – the best way out of a crisis. In the absence of alternative sources of recovery (for instance, from governmental sources), commercial considerations come to the fore. In some cases, disruption to essential services that affect many people may also mean that social harm might be reduced by paying a ransom. The ability to extract ransoms has made ransomware an extremely profitable and efficient business model. **The emergence of the cryptocurrency industry**. The development of cryptocurrency has allowed cybercriminals to pair their effective extortion tactics with the opportunity to demand difficult-to-trace ransom payments. While cryptocurrency is not impossible to trace,[35] ransomware operators and the laundering specialists they use have developed strategies to obscure the movements of funds.[36] **Professionalisation of the ransomware ecosystem**. Ransomware groups, fuelled by increased profits, have recruited more salaried employees. In contrast to independent contractors, these employees often have dedicated workstreams as part of a broader organised division of labour.[37] At the time of the so-called 'Conti leaks',[38] the organisation behind this ransomware operation employed between 65 and 100 salaried employees, with HR staff and policies.[39] This development means roles within the ecosystem have become more specialised.[40] Ransomware operators have closely collaborated with the broader cybercriminal ecosystem, particularly individuals, organisations and marketplaces that specialise in obtaining and selling access to victim networks – so-called 'initial access' brokers and markets – and specialists in laundering cryptocurrency.[41]

35. In theory, at least, it is very transparent.
36. Intel471, 'How Cryptomixers Allow Cyber-Criminals to Clean Their Ransoms', 15 November 2021, <https://intel471.com/blog/cryptomixers-ransomware>, accessed 3 March 2022.
37. Brian Krebs, 'Conti Ransomware Group Diaries, Part II: The Office', *Krebs on Security*, 2 March 2022, <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/>, accessed 3 March 2022.
38. In February 2022, a Ukrainian researcher leaked internal chat logs belonging to the organisation behind Conti and other cybercriminal enterprises. See John Fokker and Jambul Tologonov, 'Conti Leaks: Examining the Panama Papers of Ransomware', Trellix, 31 March 2022, <https://www.trellix.com/en-gb/about/newsroom/stories/research/conti-leaks-examining-the-panama-papers-of-ransomware.html>, accessed 31 December 2022.
39. Sakellariadis, 'Behind the Rise of Ransomware'.
40. Peter Grabosky, 'The Evolution of Cybercrime, 2006–2016', in Holt (ed.), *Cybercrime Through an Interdisciplinary Lens*, pp. 22–23; Jonathan Lusthaus, Jaap van Oss and Philipp Amann, 'The Gozi Group: A Criminal Firm in Cyberspace?', 2022, p. 10.
41. ENISA, 'ENISA Threat Landscape 2021: April 2020 to Mid-July 2021', October 2021, p. 26; David S Wall, 'Cybercrime as a Transnational Organized Criminal Activity', in Felia Allum and Stan Gilmour (eds), *Routledge Handbook of Transnational Organized Crime*, 2nd edition (Abingdon: Routledge, 2022), p. 331.

Drivers	Enablers
Poor cyber security practices among organisations	**The difficulties of securing modern IT infrastructure**. As one prominent cyber security practitioner said in relation to ransomware, 'cyber security is hard'.[42] The widespread reliance on technology that often prioritises ease of use over secure configurations and the difficulties of maintaining and patching critical hardware and software have enabled ransomware operators to monetise the conditions of modern information technology.[43] **Commercial and informational barriers to investment in cyber security**. Among organisations of all sizes, but particularly SMEs, the lack of an obvious commercial rationale and the intangible nature of cyber risk limit investment in cyber security. Among SMEs, there is also a strong sense that ransomware attacks only happen to large organisations.[44] Media reporting compounds this, as it tends to focus on attacks against critical national infrastructure, large corporations or geopolitically significant events.
The low-cost nature of the cybercriminal ecosystem	**Permissive law enforcement environments, mainly in Russia**. Russian government interaction with the cybercriminal ecosystem is one of the main enablers of global financially motivated ransomware.[45] The motivations most often attributed to Russia in providing safe harbour for cybercriminals are to achieve geopolitical aims and to sustain a highly capable domestic cybercriminal ecosystem it can draw on when needed.[46]

Source: Author generated.

Taken together, these drivers have helped create a low-cost, high-reward criminal enterprise. This has made ransomware, to paraphrase one Russian initial access broker, more addictive than heroin for cybercriminals.[47] Weaning the cybercriminal ecosystem off the ransomware drug involves changing the risk–reward calculus of ransomware operators and affiliates.

42. Kevin Beaumont, 'The Hard Truth About Ransomware: We Aren't Prepared, it's a Battle With New Rules, and it Hasn't Near Reached Peak Impact', DoublePulsar, 8 June 2021, <https://doublepulsar.com/the-hard-truth-about-ransomware-we-arent-prepared-it-s-a-battle-with-new-rules-and-it-hasn-t-a93ad3030a54>, accessed 3 March 2022.
43. *Ibid.*
44. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 34.
45. Ransomware Task Force, 'Combating Ransomware', p. 17; Chainalysis, 'Ransomware 2021: Critical Mid-Year Update', July 2021, p. 3.
46. US Department of the Treasury, 'Treasury Sanctions Russia with Sweeping New Sanctions Authority', press release, 15 April 2021, <https://home.treasury.gov/news/press-releases/jy0127>, accessed 3 March 2022.
47. Dmitry Smilyanets, 'An Interview With Initial Access Broker Wazawaka: "There Is No Such Money Anywhere as There is in Ransomware"', *The Record*, 26 August 2022, <https://therecord.media/an-interview-with-initial-access-broker-wazawaka-there-is-no-such-money-anywhere-as-there-is-in-ransomware/>, accessed 29 December 2022.

The Cyber Insurance Market and Ransomware

Finally, it is worth briefly explaining how cyber insurance provides coverage for ransomware and how the market has evolved over the past several years. If organisations and governments were unprepared for the rise of ransomware, the same is true of the cyber insurance industry.

Cyber Insurance Coverage for Ransomware

Cyber insurance policies first emerged in the 1990s to fill the gaps in existing insurance lines. The development of cyber insurance was largely driven by concerns in the US about liabilities related to new legislation and regulation to protect personal data. Over time, cyber insurance products offered an expanding range of policies, including, but not limited to, coverage for: first- and third-party exposures; business interruption; third-party liabilities; data and software loss; and regulatory notification costs.[48]

Insurers also began to provide coverage for cyber extortion and ransomware through standalone cyber insurance products. Although cyber extortion was initially covered by existing kidnap and ransom policies, this practice declined in the 2010s.[49] In 2020, an OECD analysis of 35 standalone cyber insurance products found that all offered some form of coverage for cyber extortion or ransomware.[50] Cyber insurance policies typically cover the external expenses associated with a ransomware attack, business interruption costs, liabilities to third parties affected by the attack and any ransom paid. However, as the next section highlights, coverage limits for ransomware specifically have become more limited.

Cyber insurers also provide access to and indemnify the costs of ransomware response services such as digital forensics and incident response, crisis management, legal services, ransomware negotiators and credit monitoring services.[51] Obtaining access to these services, particularly for SMEs, became and remains a major selling point for cyber insurance.[52]

48. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 7.
49. Tom Baker and Anja Shortland, 'Insurance and Enterprise: Cyber Insurance for Ransomware', *Geneva Papers on Risk and Insurance–Issues and Practice* (2022).
50. OECD, 'Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation', 2020, <https://www.oecd.org/pensions/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf>, accessed 4 March 2022.
51. See Annex 2 for more details about ransomware response services provided by cyber insurance policies.
52. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'.

Typically, these services are made available through what is routinely described as a 'panel', collating specific firms that the insurer has preapproved.[53] When responding to a ransomware incident, insureds will typically access these services through a hotline operated by a third-party law firm or external claims handler, which triages the incident and recommends specific firms based on the size and severity of the incident. Although some insurers have brought this process in house to monitor the claims process more closely, the 'lawyer-led' model of incident management dominates the cyber insurance industry.[54]

The role of cyber insurance in providing access to ransomware response services has two important implications. First, it highlights how insurers have considerable influence in shaping which ransomware response firms insureds can access and, by extension, the way they respond to ransomware attacks. Indeed, cyber insurance acts a form of governance on the response ecosystem: concentrating work with specific firms, negotiating discounted rates and withdrawing future work from providers who do not meet expectations.[55] At the same time, insurers' involvement does not typically extend to direct influence over incident management once an insured has contracted response services.

Second, as others have noted, lawyers play a significant role in coordinating and leading the response to ransomware attacks.[56] This is partly a legacy of the early 2010s, when data breaches and personal data theft were the biggest risks for insureds, as lawyers specialise in minimising liability risk from potential data breach litigation and can cloak the response within legal professional privilege.[57] The influence of lawyers has endured in the ransomware age, giving them an outsized influence on victim decision-making and attack response.

The Shift From a Soft to a Hard Market

Until 2019, ransomware did not register as a major problem for the cyber insurance market. The cyber insurance market was characterised as 'soft' until late 2020.[58] A steady growth of profits for early entrants to the market in the 2000s brought a new influx of insurers and capacity in the 2010s, creating what one ex-cyber insurance underwriter described as a 'mad cash rush',[59] and another as a 'gravy

53. Daniel Woods and Rainer Bohme, 'How Cyber Insurance Shapes Incident Response: A Mixed Methods Study', paper presented at the 20th Annual Workshop on the Economics of Information Security, 28 June 2021, p. 5.
54. *Ibid.*, pp. 10–12.
55. *Ibid.*, p. 20.
56. *Ibid.*; Baker and Shortland, 'Insurance and Enterprise: Cyber Insurance for Ransomware'.
57. *Ibid.*
58. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 26.
59. Insurance industry association 3, 24 November 2021.

train'.[60] This led to fierce competition to grow market share, with a race to the bottom in pricing and brokers able to negotiate broader coverage terms and limits for their clients.[61] The result was a growing disconnect between pricing and risk, with premiums more sensitive to market competition than to the mounting threat of ransomware. Even as losses started to build up, the initial market response was, according to one ex-cyber insurance industry executive, 'essentially to absorb losses early on, because everybody was still worried about market share'.[62]

The race to the bottom was also characterised by minimal security requirements to obtain coverage. Although early cyber underwriters undertook extensive security assessments, these were abandoned as competition in the market increased.[63] This led to a situation where insurers had neither carrots (financial incentives for installing security controls or using pre-breach services) nor sticks (security obligations in policies) to improve the risk posture of policyholders.[64] Insurers that wanted to do things differently found themselves undercut by brokers who could obtain coverage from competitors who would simply offer coverage without the same security requirements. Some underwriters interviewed as part of the research were damning about the consequences of this: 'you could see a risk five years ago which had the worst controls you've ever seen, say no to everything on the application form and it would still get the insurance'.[65] Meanwhile, many businesses had – and continue to have – no cover at all.

These market conditions created a perfect storm for insurers as ransomware attacks and payments grew.[66] Ransomware introduced significant business interruption losses for insurers on a frequent basis. As one actuary noted in an interview, 'the moment ransomware brought business interruption, the world went crazy'.[67] This was compounded by the fact that most insureds did not have credible offline backups that would allow them to reduce business interruption costs, pushing them to either pay ransoms or face extended outages.[68] From Q1 2019 to Q4 2021, the insurance broker Aon recorded a 323% increase in ransomware

60. DFIR 9, 4 February 2022.
61. Insurance industry association 1, 29 October 2021.
62. Insurance industry association 3, 24 November 2021.
63. Woods, 'The Evolutionary Promise of Cyber Insurance'.
64. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'.
65. Cyber insurance underwriter, RUSI workshop, 17 February 2022; cyber insurance underwriter 4, 21 October 2021; cyber security consultant 1, 24 September 2021; MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'; Woods and Moore, 'Does Insurance have a Future in Governing Cybersecurity?'.
66. Insurance industry association 2, 17 November 2021.
67. Cyber risk analytics 1, 28 October 2021.
68. Claims manager, RUSI workshop, 17 February 2022.

claims among its clients.[69] One industry report suggested that ransomware claims made up 75% of all cyber insurance claims in the US market in 2020.[70] This dramatic rise in claims and losses turned cyber insurance from a profitable line to a loss-making one for many of the largest US carriers in 2020 and 2021.[71]

Many insurers have changed tack in response to these losses. Since at least early 2021, the cyber insurance market has been characterised as 'hard'. In practice, this has resulted in increased premiums, reduced coverage, increased security requirements, and exclusions and sub-limits. Put simply, the cost of policies and the requirements for purchasing them have risen.[72] Although these conditions can make purchasing cyber insurance more difficult for organisations, the hardening market also creates opportunities from a public policy perspective. Insurers currently have clear financial incentives to reduce the risk from ransomware or they could be forced to exit the market entirely.[73] Limited market penetration of cyber insurance means that policymakers must also be realistic about its potential to shape the ransomware challenge, whether for better or worse, at scale.[74]

With this in mind, the next three chapters explore the potential role of cyber insurance in disrupting some of the drivers and enablers of ransomware.

69. Aon, 'E&O and Cyber Market Review', 2022, <https://publications.aon.com/eo-and-cyber-market-review/loss-and-pricing-trends>, accessed 5 March 2022.
70. AM Best, 'Best's Market Segment Report: Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk', 2 June 2021, <https://news.ambest.com/presscontent.aspx?refnum=30762&altsrc=9>, accessed 6 March 2022.
71. *Insurance Journal*, 'Top 20 Cyber Insurers in the US, Including Loss Ratios', 9 November 2021, <https://www.insurancejournal.com/news/national/2021/11/09/641279.htm>, accessed 7 March 2022; R J Dumaual and Husain Rupawala, 'Cyber Underwriters' Premiums Surge, Loss Ratios Improve in '21', *S&P Global*, 10 May 2022.
72. For more details on these market conditions, see Gareth Mott et al., 'Between a Rock and a Hard(ening) Place: Cyber Insurance in the Ransomware Era', *Computers and Security* (Vol. 128, 2023), pp. 6–7.
73. Eric Cho, 'Why the Hardening Cyber Market Benefits All', *Asia Insurance Review*, August 2021, <https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle?aid=44731>, accessed 9 August 2022.
74. The most recent UK government cyber breaches survey, for instance, highlighted that only 30% of businesses have some sort of cyber insurance coverage, and only 7% have a dedicated policy. See Department for Science, Innovation and Technology, 'Cyber Security Breaches Survey 2023', 19 April 2023.

II. The Role of Cyber Insurance in the Ransomware Business Model

Ransomware is a high-reward criminal enterprise that has made at least several billion dollars at the time of writing.[75] Some argue that insurers have normalised ransom payments and created a form of moral hazard by indemnifying them, leading to inflated payments and increasing rewards for cybercriminals. Yet insurers also have a financial interest in stabilising and reducing the profitability of the ransomware business model and have the potential to shape insureds' decision-making in more positive ways.

Research conducted for this report paints a nuanced picture. For victims, the decision to pay a ransom is a complex dilemma involving many factors, and it is rarely a silver bullet. Crucially, there is no strong evidence that insurers are encouraging victims to pay ransoms. In fact, it seems likely that most ransomware victims with cyber insurance make more informed decisions about ransom payments and generally handle incidents better than those without insurance. At the same time, the potential role that cyber insurance could play in actively reducing the profitability of ransomware is limited by a lack of market-wide best practices for ransomware response, a lack of clarity over what constitutes a reasonable last resort for a ransom payment, and limited market penetration.

The Ransom Payment Debate

At the heart of the ransomware challenge is the issue of incentives around ransom payments. As the ransomware challenge has grown in scale and impact, victims have been forced to make difficult decisions about whether to pay ransoms to potentially regain access to critical systems or protect stolen data.

75. FinCEN, 'FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021', 1 November 2022, <https://www.fincen.gov/news/news-releases/fincen-analysis-reveals-ransomware-reporting-bsa-filings-increased-significantly>, accessed 31 July 2023.

Paying a ransom often makes sense – or is even essential – from an organisational perspective. Faced with several weeks or months of downtime and the resulting financial losses, many victims will choose to pay the ransom even though recovery is not guaranteed. These motivations can be even stronger in critical national infrastructure, where the choice may be between maintaining delivery of essential services or paying a ransom.

However, paying a ransom also increases the risk of future attacks and can encourage ever larger extortions if victims agree to inflated demands. The position of the UK and many other governments on ransomware payments has been clear, at least publicly. They do not want victims to pay, and argue that this fuels the problem and does not guarantee the return of data.[76] However, this glosses over the complexities victims face when responding to ransomware, and does not offer victims tangible alternatives to payment.[77] In practice, the current approach also means that citizens and private companies make decisions on ransoms that have a myriad of societal and public policy, as well as commercial, consequences.

Amid the broader debate on ransom payments, there has also been significant criticism levelled at the insurance industry. Although the dilemma around whether to pay a ransom exists regardless of whether a victim is insured, many policymakers, researchers and cyber security practitioners have argued that access to cyber insurance increases the propensity to pay.[78] Proponents of this argument offer two main reasons:

1. Because it is often believed to be less painful and costly to pay a ransom than to deal with prolonged business interruption or potential liability costs from data exposure, insurers advise or encourage victims to pay ransoms.[79]

76. NCSC, 'Ransomware', <https://www.ncsc.gov.uk/ransomware/home#section_3>, accessed 31 July 2022; NCSC, 'Lindy Cameron Speaking at the RUSI Annual Security Lecture', 14 June 2021, <https://www.ncsc.gov.uk/speech/rusi-lecture>, accessed 5 August 2022.
77. For a nuanced articulation of this point, see Tarah Wheeler and Ciaran Martin, 'Should Ransomware Payments be Banned?', Brookings, 26 July 2021.
78. Dan Sabbagh, 'Insurers "Funding Organised Crime" by Paying Ransomware Claims', *The Guardian*, 24 January 2021; Jan Lemnitzer, 'Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help', *The Conversation*, 8 March 2021; Renee Dudley, 'The Extortion Economy: How Insurance Companies are Fuelling a Rise in Ransomware Attacks', *ProPublica*, 27 August 2019, <https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks>, accessed 20 October 2022; Josephine Wolff, 'As Ransomware Demands Boom, Insurance Companies Keep Paying Out', *Wired*, 12 June 2021; Kyle D Logue and Adam B Shniderman, 'The Case for Banning (and Mandating) Ransomware Insurance', University of Michigan Law and Economics Working Papers, No. 207, 18 August 2021; O'Ryan Johnson, 'CISA Leader Tells MSPs Cyber Insurance Market "Fuelled Rise in Ransomware"', *CRN*, 24 February 2023, <https://www.crn.com/news/channel-news/cisa-leader-tells-msps-cyber-insurance-market-fueled-rise-in-ransomware->, accessed 8 March 2023.
79. Lemnitzer, 'Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help'; Dudley, 'The Extortion Economy'; Wolff, 'As Ransomware Demands Boom, Insurance Companies Keep Paying Out'.

2. Access to liquidity through cyber insurance coverage, particularly for SMEs, makes paying the ransom easier for organisations with insurance than for those without.[80] This also causes ransom inflation because access to high policy limits makes it easier for insureds to accede to outsized ransom demands.

This perspective suggests that cyber insurance is making the ransomware business model more profitable because victims with insurance are more likely to pay. In interviews, policymakers and law enforcement officers suggested several times that they believe cyber insurance is fuelling ransom payments.[81]

On the other hand, it is also possible that cyber insurance can stabilise the growth of ransom payments, enable victims to make informed decisions, and disincentivise them from paying the kind of outsized demands that encourage more criminals to join the ecosystem. In her book on the kidnap-for-ransom market, Anja Shortland characterises this approach as one that creates 'ransom discipline'.[82] This highlights the potential of cyber insurance to reduce the profitability of the ransomware business model – not by stopping all ransom payments, but by creating a stable and more tightly governed market for them.

The Effects of Cyber Insurance on Ransom Payments

Interviewees and workshop participants expressed a range of views on how cyber insurance affects both victim and attacker decision-making about ransom payments. Using thematic analysis, we identified eight ways in which cyber insurance does (or, in some cases, does not) have an effect on ransom payments.

Insurers Do Not Make Decisions About Ransom Payments for Insureds

Interviewees were almost unanimously of the view that insurers do not advise victims to pay or not pay ransoms. As one director at an incident response firm made clear, 'I've never seen that, in many hundreds of situations'.[83] This was echoed by a UK-based lawyer who suggested 'In my career, I've never experienced

80. Logue and Shniderman, 'The Case for Banning (and Mandating) Ransomware Insurance'.
81. Government 2, 1 December 2021; government 3, 1 December 2021; government 4, 10 January 2022; law enforcement 2, 3 November 2021.
82. Anja Shortland, *Kidnap: Inside the Ransom Business* (Oxford: Oxford University Press, 2019), pp. 108–09. For a recent RUSI report comparing the cyber insurance and kidnap-for-ransom markets, see Shortland, Keatinge and MacColl, 'Insurance as Crime Governance'.
83. DFIR 6, 23 November 2021.

an insurer saying, "we want you to pay a ransom because it'll cost us, the insurer, less in the long run"'.[84] This was even true of incident response and cyber security practitioners who believe that the insurance industry has fuelled ransomware.

The most prominent and well-cited counter to this perspective is a 2019 ProPublica article, which covered the story of a ransomware attack against the local government of Lake City, Florida.[85] According to the article, the city's insurer conducted a cost–benefit analysis and recommended that the government pay the ransom rather than pursue an alternative and potentially more costly approach. A city spokesperson concluded at the time, 'our insurance company made the decision for us'.[86]

It is undoubtedly true that many insurers, which are part of a for-profit industry after all, prefer the most cost-effective outcomes. In some cases, this may mean paying the ransom rather than extended business interruption. 'As an insurer', suggested one broker, 'if your client chooses not to pay that ransom, quite often it can cost us a lot more money because we don't get the solution'.[87] In other cases, it may mean a preference against paying ransom payment. Indeed, several interviewees noted that as ransom demands have increased in the past several years, the business case for paying the ransom has become less compelling for both insurers and insureds.[88] According to some underwriters, this is particularly true in the case of medium-sized victims, where ransom demands can be greater than the costs associated with several weeks of downtime.[89] This suggests that as ransom demands have become more inflated, the cost–benefit analysis has shifted away from paying in at least some cases. However, how claims teams or third parties conduct cost–benefit analyses is unclear, and may be an art rather than a science.

Although insurers may, to some extent, be involved in deciding who is in the room, given their ability to appoint firms to panels, they are largely removed from the crisis management group that provides guidance to executive leadership around the pros and cons of paying a ransom. As an interviewee from a ransomware response and recovery firm argued, 'they're not really in the room' when it comes to decision-making.[90] One interviewee with direct involvement

84. Breach counsel 2, 9 December 2021.
85. Dudley, 'The Extortion Economy'.
86. *Ibid.*
87. Broker 5, 8 December 2021.
88. Underwriter 7, 2 November 2021; cyber insurance underwriter 2, 15 October 2021; DFIR 4, 27 October 2021.
89. Underwriter 7, 2 November 2021; cyber insurance underwriter 2, 15 October 2021.
90. Ransomware recovery 1, 3 November 2021. This point was echoed by insurance industry association 1, 29 October 2021; DFIR 5, 1 November 2021; DFIR 7, 9 December 2021; cyber insurance broker 5, 8 December 2021; DFIR 6, 23 November 2021; cyber insurance broker 1, 12 November 2021; DFIR 3, 21 October 2021.

in the Lake City ransomware attack emphasised that the insurer was not involved in any decision-making meetings, and that an external counsel provided guidance around the ransom payment.[91] According to this individual, 'the [spokesperson] that said they were told to do certain things by the insurance company was [mistaken] … they were told to do certain things by their lawyer, and there were so many people on the call that they didn't know who was who'.[92]

Even the minority of insurers that have a more active role in managing claims or coordinating ransomware response services – or even joining client calls – only provide guidance around options, rather than providing direct advice on whether to pay.[93] In fact, some insurers suggested that they have far less influence on insureds than they would like.[94]

This does not rule out the possibility that insurers' preferences are reflected in the guidance that the ransomware response services – particularly external counsel, incident response and negotiators – provide through panels. However, arguments that insurers encourage or compel victims to pay on the basis of cost misunderstand the nature of their influence on victim decision-making.

Payment Authorisation as a 'Last Resort'

Although insurers do not typically provide direct advice to insureds on whether or not to pay a ransom, they do have some influence over the final payment.[95] In today's market, most coverage of ransom payments is reimbursement coverage – in other words, insurers do not pay the ransom directly. Many policies are affirmative, which means insureds require written consent from the insurer before they can make a payment and secure reimbursement.[96] Other policies leave the decision to the insured but include language to the effect that ransom payment must be necessary, reasonable and legal.[97] It is also important to note that policies do not require the insurer's consent if an insured chooses not to pay the ransom but instead recover via other means.[98]

How does this impact victims' decision-making? A common refrain from insurers was that they only authorise payments as a 'last resort'. What this means in

91. The footnote for this interviewee has been removed to preserve anonymity.
92. *Ibid*.
93. Claims 1, 24 September 2021; DFIR 5, 1 November 2021; cyber insurance claims 2, 11 October 2021; cyber insurance claims 3, 1 December 2021.
94. Broker 1, 12 November 2021; cyber insurance claims 1, 24 September 2021; cyber insurance underwriter 9, 1 December 2021.
95. Logue and Shniderman, 'The Case for Banning (and Mandating) Ransomware Insurance'.
96. Breach counsel 1, 12 November 2021; cyber insurance claims 1, 24 September 2021.
97. Claims 1, 24 September 2021.
98. Darren Pain and Dennis Noordhoek, 'Ransomware: An Insurance Market Perspective', Geneva Association, July 2022, p. 24.

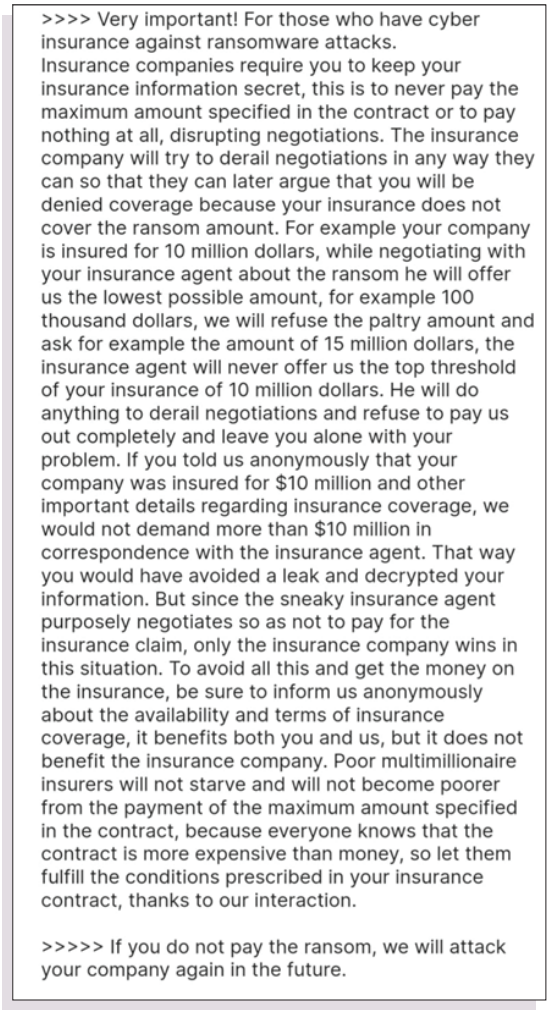
practice varies significantly by policy and insurer. As one claims manager at a US insurer suggested, 'the policy forms across markets tend not to define what kind of steps would be needed to be taken in much detail to secure coverage for a ransomware payment'.[99] For some insurers more actively involved in the claims management process, there is a growing tendency towards requiring reporting to law enforcement and clear evidence that the insured has worked through opportunities to recover through other means before authorising a payment.[100] However, what constitutes a 'last resort' appears opaque and subjective in many cases, and there are few developed protocols for how to reach this point in practice.

The effect of this is that ransom payments are mostly authorised by insurers – with the exception of incidents where sanctions may be violated.[101] 'If the decision's made to pay a ransom', one US broker suggested, 'I've yet to see an insurer say, "no, we disagree"'.[102] This reinforces the point that the decision lies with the insured. It also does not rule out that insurers and ransomware response services guide towards payment as a 'last resort', rather indicating that most insurers do not have the contractual levers to ensure this happens.

Our interviews highlighted that some insurers have become more active in only authorising payments after the ransom amount has been negotiated to an acceptable level. Incident response and ransomware negotiation specialists highlighted that some claims handlers are much more actively involved in monitoring negotiations to ensure costs are brought down before they authorise a payment.[103] Some ransomware operators have also noted this. The ransom note accompanying the latest strain of LockBit ransomware, for instance, advises victims that 'sneaky' insurers 'never pay the maximum amount specified in the contract … disrupting negotiations'.[104] This may indicate that insurers are finding ways to ensure outsized ransom demands are not paid.

99. Claims 1, 24 September 2021.
100. Claims 1, 24 September 2021; cyber insurance underwriter 7, 2 November 2021.
101. Claims 3, 1 December 2021; DFIR 6, 23 November 2021; cyber insurance broker 1, 12 November 2021; DFIR 9, 4 February 2022; DFIR 3, 21 October 2021; DFIR 7, 9 December 2021.
102. Broker 1, 12 November 2021.
103. DFIR 3, 21 October 2021; DFIR 6, 23 November 2021; ransomware negotiation specialist, RUSI workshop, 17 February 2022.
104. Thomas Meskauskas, 'LockBit 3.0 Ransomware Virus', PCrisk, 22 November 2022, <https://www.pcrisk.com/removal-guides/24242-lockbit-3-0-ransomware>, accessed 9 July 2023.

Figure 2: LockBit Ransom Note



Source: Thomas Meskauskas, 'LockBit 3.0 Ransomware Virus', PCrisk, 22 November 2022, <https://www.pcrisk.com/removal-guides/24242-lockbit-3-0-ransomware>, accessed 9 July 2023.

Cyber Insurance and Crisis Management

Cyber insurance has forms of influence beyond providing ransom payment coverage. Indemnifying recovery costs other than the ransom provides a financial safety net which may lessen the incentive to pay or increase the time available to victims to consider their approach to recovery or negotiations. Access to ransomware response services may also help victims understand the options available to them.

Options

Cyber insurance may lessen the incentive to pay unnecessary or inflated ransoms by increasing options and expertise through access to ransomware response

services. For organisations that do not have these services on retainer, cyber insurance facilitates access to a crisis management function that can help create order and structure for victims. This provides access to specialists with accrued knowledge and expertise that many – particularly smaller organisations – would otherwise struggle to know how to access.[105] In theory, insurers' claims hotlines will also help connect insureds with the most suitable firms based on their requirements and circumstances.[106]

Ransomware response specialists can help victims explore alternatives to paying a ransom. Examples of this include identifying publicly available decryption keys for different ransom strains, exploring alternative ways to recover and remediate backups, and investigating the credibility of threats from data exposure. Incident response firms with strong relationships with law enforcement agencies may encourage reporting, which can also increase victims' options if law enforcement agencies have access to additional decryption keys or other alternatives to payment.[107] Taken together, this suggests that access to ransomware response services provides at least some mechanisms for victims to avoid paying or making a payment as a last resort. However, the influence of insurance on this is likely to be more of a factor for SMEs than for large organisations. Interviewees from large financial services, technology, transport and defence firms all highlighted that they already retained access to these types of services. They did, however, acknowledge the value of insurance as a facilitator of ransomware response for smaller organisations.[108]

Time

Access to insurance may also increase the time for victims to explore alternatives to payment by providing financial security through coverage of business interruption costs and access to specialist services. As one claims manager with a background in technical incident response highlighted, this can alter the calculus around whether to pay, as 'it gives [victims] a chance to take a step back and evaluate what's really going on and not rush themselves into a decision to pay a ransom quickly … we know [that] when people panic, they make poor

105. DFIR 5, 1 November 2021; cyber insurance executive 1, 11 October 2021; breach counsel 2, 9 December 2021; Breach counsel, RUSI workshop, 17 February 2022.
106. Woods and Bohme, 'How Cyber Insurance Shapes Incident Response'.
107. Breach counsel 2, 9 December 2021; ransomware recovery 1, 3 November 2021; ransomware recovery and negotiation specialist, RUSI workshop, 17 February 2022; US Department of Justice, 'US Department of Justice Disrupts Hive Ransomware Variant', 26 January 2023, <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>, accessed 30 January 2023.
108. Technology 1, 10 November 2021; technology 2, 10 November 2021; financial services 1, 28 October 2021; defence 1, 16 November 2021; transport 1, 11 November 2021; cyber risk manager at a financial services firm, RUSI workshop, 17 February 2022.

decisions'.[109] This was validated by a senior director from a specialist ransomware recovery firm that has managed hundreds of negotiations: 'what we see is if the decision to pay a ransom can be delayed even just a few days, the likelihood of paying a ransom comes down'.[110] One quantitative analysis of ransomware also suggests that delaying a decision around payment may nudge victims away from paying.[111] This highlights that insurance can help create conditions for a better crisis management process, particularly for SMEs that are unlikely to have ready access to these kinds of services.

Cyber Insurance and Sanctions Compliance

Organisations with insurance – particularly SMEs – may be more cognisant of US and UK sanctions targeted at certain ransomware strains, cryptocurrency wallets or specific criminals.[112] This means that insurance can help to increase sanctions compliance and potentially reduce the number of ransoms paid to sanctioned entities.

Some specialist ransomware payment firms, which are usually responsible for ransomware due diligence, use threat intelligence and data on behavioural patterns to assess sanctions risks.[113] External counsels are also sensitive to the possibility of breaking US law.[114] Given at least some ransomware payment firms are registered as money services businesses in the US,[115] this means they also have to comply with reporting requirements from the US Treasury Financial Crimes Enforcement Network (FinCEN) and FATF (Financial Action Task Force) red flags.[116] However, it is not clear if this is the case for all payment firms.

Insurers themselves also influence victims' decision-making around sanctions. As tightly regulated entities bound by additional standards and scrutiny, they are not able to reimburse payments to criminal or state actors suspected of being sanctioned, and similarly would not receive their own reimbursement payment

109. Claims 3, 1 December 2021.
110. RUSI workshop, 17 February 2022.
111. Bakuei Matsukawa et al., 'Ransomware as a Science', paper presented to FIRSTCON 22, 34th Annual Conference, Dublin, 26 June–1 July 2022, <https://www.first.org/resources/papers/conf2022/FIRST22_RansomwareasaScience_TLP_WHITE_WITHOUT_SOME_SLIDES.pdf>, accessed 7 October 2022.
112. US Department of the Treasury, 'Updated Advisory on Potential Risks for Facilitating Ransomware Payments', 21 September 2021, <https://ofac.treasury.gov/media/912981/download?inline>, accessed 8 July 2023.
113. Claims 3, 1 December 2021; ransomware recovery 1, 3 November 2021; ransomware recovery specialist, RUSI workshop, 17 February 2022; Richard Vanderford, 'Russia Sanctions Complicate Paying Ransomware Hackers', *Wall Street Journal*, 28 April 2022.
114. Breach counsel 1, 6 December 2021.
115. *Ibid.*
116. Kivu, 'Counter Extortion and Threat Intelligence', <https://kivuconsulting.com/counter-extortion-threat-intelligence/>, accessed 8 July 2022; Coveware, 'Privacy Policy', last updated March 2022, <https://www.coveware.com/privacy-policy>, accessed 8 July 2022.

from reinsurers. The insurance industry is also increasing efforts to formalise ransomware sanctions due diligence. In December 2021, the Lloyd's Market Association released a detailed checklist for insurers and insureds to follow to ensure compliance with sanctions.[117] At least one insurer has also developed their own tool for assessing sanctions risks related to threat actors and cryptocurrency wallets.[118]

At the same time, several interviewees from the insurance industry and incident response firms highlighted that due diligence for ransomware sanctions is an imperfect system. One former cyber insurance executive suggested that insurers have been anxious about not reimbursing ransom payments where a sanctioned entity is suspected, because of possible litigation by insureds: 'the carriers are more fearful of those bad faith claims than paying any individual ransom payment'.[119] An executive from a cyber reinsurer also highlighted that although it is possible to prevent payments to sanctioned entities, 'when it has not been possible to attribute … people tend to default to it being a non-sanctioned entity, so claims are made'.[120] However, it is still reasonable to generalise that victims with insurance – particularly smaller organisations – are more likely to be aware of sanctions risks than those without. Media reporting suggests this is likely to be even more true following Russia's invasion of Ukraine, with insurers and payment firms becoming more vigilant due to the growing number of sanctions targeting Russia and the ambiguity around the links between Russian ransomware operators and the Russian state.[121]

Ransomware Response Services and Ransom Discipline

As well as raising standards of crisis management and access to specialist ransomware negotiation, recovery and payment firms may also improve ransom discipline. Insurers have concentrated these services in a handful of firms, which have collectively managed at least several thousand ransomware incidents. This means they can monitor which ransomware operators provide reliable decryption keys upon payment.[122] In 2021, one recovery firm reported that 99%

117. Lloyd's Market Association, 'Guidance for Handling a Ransomware Incident', 10 December 2021, <https://www.lmalloyds.com/LMA/News/Blog/guidance_101221.aspx>, accessed 31 December 2022.
118. Cyber insurance executive 1, 11 October 2021.
119. Insurance industry association 3, 24 November 2021.
120. Cyber reinsurance executive 1, 29 November 2021.
121. Richard Vanderford, 'Russia Sanctions Complicate Paying Ransomware Hackers', *Wall Street Journal*, 28 April 2022.
122. Claims 1, 24 September 2021; cyber insurance claims 2, 11 October 2021; breach counsel, RUSI workshop, 17 February 2022.

of its clients recovered a decryption key following payment.[123] This aligns with data from Arete – an incident response firm that has been engaged on a large number of ransomware incidents and negotiations – on its experiences with obtaining decryption keys.[124] Access to these services increases the intelligence available on the reliability of ransomware operators, which in turn decreases the willingness of victims to pay less trustworthy gangs. Specialist negotiation firms should, at least in theory, also allow insureds to reduce the size of payments made to criminals by improving the quality of bargaining with threat actors.

In some cases, reputable ransomware response firms more regularly help victims to recover without paying ransoms. Coveware, for instance, highlighted that 41% of its clients paid ransom in 2022, down from 76% in 2019.[125] Although there are likely also broader drivers that explain some of these shifts – such as improved cyber resilience,[126] increased government and law enforcement intervention, and the impact of the war in Ukraine – there was a general sense in interviews and the workshop that insurers and reputable ransomware response services have made inroads in enabling victims to recover from ransomware operations that encrypt data without paying a ransom.

At the same time, some interviewees highlighted concerns about the role of some ransomware response firms in normalising or inflating payments in cases where there is a reasonable chance of recovery without paying a ransom. The quality of response services, for instance, apparently varies significantly by provider, and there are no clearly defined protocols around ransomware response – particularly negotiations.[127] There may also be mixed incentives for some ransomware negotiation and payment providers. At least one firm reportedly provides negotiations and facilitates cryptocurrency payments on behalf of clients, taking a flat fee for negotiations but a percentage of every payment.[128] There is still some way to go in creating market-wide ransom discipline, even if some insurers and response firms appear to be moving in the right direction.

123. Coveware, 'Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Demands'.
124. Cyentia Institute and Arete, 'Mitigating Ransomware's Impact, Investigative Cybercrime Series: Vol. 1', 2 June 2022, <https://areteir.com/static/e4a878b0ecf942960936161ee20009ee/mitigating-ransomwares-impact.pdf>, accessed 8 July 2022.
125. Coveware, 'Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting', 3 May 2022, <https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting>, accessed 8 July 2022.
126. The role of insurance in improving cyber security and resilience is explored in the next chapter.
127. Lawyer 1, 28 October 2021; insurance industry association 3, 24 November 2021; Shortland, Keatinge and MacColl, 'Insurance as Crime Governance'.
128. DFIR 6, 23 November 2021; insurance industry association 3, 24 November 2021; cyber insurance claims 1, 24 September 2021.

Insurance and Double Extortion

The evolution of extortion tactics by cybercriminals outlined in Chapter I has complicated the decision-making process for victims and made it more difficult for insurers to encourage ransom discipline. Although insurers and ransomware response providers are increasingly confident that they can help insureds recover from attacks that encrypt or lock data if there are sufficiently protected and up-to-date backups, the rise of data-theft-based extortion (so-called 'double extortion') as a tactic has created new incentives that drive insureds towards payments.[129] One cyber insurance claims manager remarked in the workshop that 'what's been the pinch point has generally been the threat of publishing data rather than getting data encrypted … that's what tends to force our insureds' hand in terms of ransom payments, at least over the past 12 to 18 months or so'.[130]

There are likely several incentives that drive payments in cases of data extortion. One is the potential reputational harm that may follow disclosure of sensitive commercial or personal data. These fears are often increased by the tactics that ransomware operators use to increase leverage and ramp up pressure, such as notifying media outlets, cold calling victims' employees and customers, and contacting senior executives personally. A second reason is the concern about potential harm to individuals, and associated regulatory fines and litigation costs as a result of confidential personal data being exposed.[131] A more nebulous incentive is what one incident response practitioner described as 'convenience'[132] – namely, paying 'just in case' data has been stolen. An infamous example is when JBS, a meat processing company, paid a $11 million ransom in 2021 to prevent 'potential risk' to their customers following an attack by REvil operators, even though they claimed no data had been compromised.[133]

Although there is no evidence that insurance necessarily provides victims with additional incentives to pay in cases of data extortion, several interviewees from insurers and incident response firms suggested that it can make it more difficult for them to guide victims towards paying as a 'last resort'.[134] This is not only because of the incentives outlined above, but also because it is much harder for insurers, claims adjusters or response firms to clearly calculate or articulate the cost–benefit tradeoff. 'Now we're [calculating] whether they feel shame or

129. Claims 1, 24 September 2021; cyber insurance underwriter 7, 2 November 2021; DFIR 7, 9 December 2021; cyber insurance executive 1, 11 October 2021; cyber insurance claims 3, 1 December 2021.
130. RUSI workshop, 17 February 2022.
131. Cyber insurance executive 1, 11 October 2021; DFIR 3, 21 October 2021.
132. DFIR 3, 21 October 2021.
133. JBS Foods Group, 'JBS USA Cyberattack Media Statement – June 9', 9 June 2021, <https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9>, accessed 31 January 2023.
134. Claims 1, 24 September 2021; DFIR 8, 19 January 2022; cyber insurance underwriter 2, 15 October 2021; cyber insurance underwriter 4, 21 October 2021.

embarrassment', remarked one claims manager, 'let alone privacy exposure or protection information'.[135] Indeed, a cost–benefit analysis about whether to pay a ransom becomes even more subjective and complex for double extortion than potential business interruption and recovery losses from ransomware attacks that only encrypt data.

The influence of ransomware response services on decision-making around payments in cases of data extortion is also more ambiguous. Some interviewees from incident response and ransomware negotiation firms suggested that they advise victims not to pay in these cases, not least because victims still need to notify regulators, as well as customers or individuals affected by data exposure, regardless of whether they have paid a ransom.[136] It is also much harder to assess whether a threat actor has actually deleted stolen data or shared it with other criminals,[137] meaning the risk to organisations or individuals affected by data exposure is not as clearly mitigated by paying a ransom as it is with encryption-based attacks.[138] Paying in the case of data extortion also reportedly increases the likelihood of re-extortion.[139] However, this stance may sometimes conflict with the advice insureds receive from some external counsels. One executive at an insurer, for instance, emphasised that 'being blunt, lawyers carry the whip hand these days because they provide the biggest fear factor, which is you're going to get sued or you're going to have an investigation by a regulator … they use that influence very heavily'.[140] This may be particularly true for US victims, given the more litigious environment. Although legal advice will impact victim decision-making irrespective of whether they have insurance, it may be more of a factor for victims with insurance given that lawyers play a significant role in coordinating incident response on behalf of many insurance carriers.[141]

The Role of Cyber Insurance in Ransomware Tactics and Targeting

Finally, in trying to understand the impact of cyber insurance on ransom payments, it is also important to assess how it affects the decision-making and

135. Claims 1, 24 September 2021.
136. DFIR 3, 21 October 2021; ransomware recovery 1, 3 November 2021; cyber insurance underwriter 2, 15 October 2021; cyber insurance underwriter 4, 21 October 2021.
137. Coveware, 'Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting'.
138. Information Commissioner's Office (ICO) and NCSC, 'Joint ICO and NCSC Letter to the Law Society and Bar Council', 7 July 2022, <https://www.ncsc.gov.uk/files/Joint-ICO-and-NCSC-letter-to-The-Law-Society-and-The-Bar-Council-V1.pdf>, accessed 8 July 2023.
139. Coveware, 'Ransomware Demands Continue to Rise as Data Exfiltration Becomes Common, and Maze Subdues', 4 November 2020, <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>, accessed 2 August 2022; Cyentia Institute and Arete, 'Mitigating Ransomware's Impact', p. 13.
140. Cyber insurance executive 1, 11 October 2021; cyber security consultant 2, 4 October 2021.
141. Woods and Bohme, 'How Cyber Insurance Shapes Incident Response'.

tactics of cybercriminals. Indeed, a recurring criticism of the role of cyber insurance in the ransomware challenge is that cybercriminals purposely target organisations with cyber insurance policies and use stolen policy documents to negotiate more profitable extortion payments.[142]

Targeting and Victim Selection

A number of interviewees argued that ransomware operators and affiliates specifically compromise organisations with cyber insurance.[143] These assessments are partly based on interviews with ransomware operators conducted by cyber threat intelligence analysts.[144] In a 2021 interview, for instance, a prominent ransomware operator associated with REvil described victims with cyber insurance as 'one of the tastiest morsels'.[145] Successful ransomware attacks against insurance companies have also fuelled speculation that ransomware operators and affiliates may be using stolen data on policyholders to guide future attacks.[146] To assess these claims, it is necessary to understand how ransomware affiliates gain access to organisations and what motivates their victim selection and prioritisation.

Ransomware affiliates either gain access to organisations themselves or use specialist access brokers that operate in the cybercriminal ecosystem. In either case, organisations are typically compromised through opportunistic tactics and techniques. These include:

- **Phishing campaigns**: malicious emails distributed by botnets that deliver malware designed to steal access credentials or drop additional malware and tools to escalate privileges.[147]

142. Samuel Greengard, 'The Double-Edged Sword of Cybersecurity Insurance', *Dark Reading*, 10 November 2020, <https://www.darkreading.com/edge-articles/the-double-edged-sword-of-cybersecurity-insurance>, accessed 23 October 2022.
143. Law enforcement 2, 3 November 2021; cyber security consultant 1, 24 September 2021; cyber security consultant 3, 4 October 2021; cyber insurance broker 3, 1 December 2021.
144. Azim Khodjibaev, Dymtro Korzhevin and Kendall McKay, 'Interview with a LockBit Ransomware Operator', Talos, 2 February 2021, <https://blog.talosintelligence.com/interview-with-lockbit-ransomware/>, accessed 29 December 2022; Dmitry Smilyanets, '"I Scrounged Through the Trash Heaps… Now I'm a Millionaire": An Interview With REvil's Unknown', *The Record*, 16 March 2021, <https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/>, accessed 29 December 2022.
145. Smilyanets, '"I Scrounged Through the Trash Heaps… Now I'm a Millionaire"'.
146. Cyber security consultant 1, 24 September 2021; cyber security consultant 3, 4 October 2021.
147. Selena Larson, Daniel Blackford and Garrett G, 'The First Step: Initial Access Leads to Ransomware', Proofpoint, 16 June 2021, <https://www.proofpoint.com/uk/blog/threat-insight/first-step-initial-access-leads-ransomware>, accessed 28 July 2022; Cybereason, 'All Paths Lead to Cobalt Strike – IcedID, Emotet and QBot', 10 February 2022, <https://www.cybereason.com/blog/threat-analysis-report-all-paths-lead-to-cobalt-strike-icedid-emotet-and-qbot>, accessed 22 July 2022.

- **Scanning for RDP instances**: a tactic that uses scanning tools to find internet-facing RDP instances to gain remote access to networks.[148] This may involve scanning for RDP instances that have been misconfigured or using stolen access credentials obtained through other means.
- **Exploiting vulnerabilities in internet-facing IT infrastructure**: in recent years, ransomware operators have exploited unpatched vulnerabilities in remote access gateways such as VPNs. By scanning for these vulnerabilities, they can identify multiple vulnerable organisations at a time.[149] Initial access brokers also gain access to remote access gateways, which they can then sell on to ransomware operators and affiliates to exploit.

These tactics and techniques are largely not targeted at specific victims but are designed to gain access to a wide range of organisations. In other words, to infiltrate organisations, ransomware affiliates and initial access brokers use opportunistic methods that are not designed to identify victims with cyber insurance.

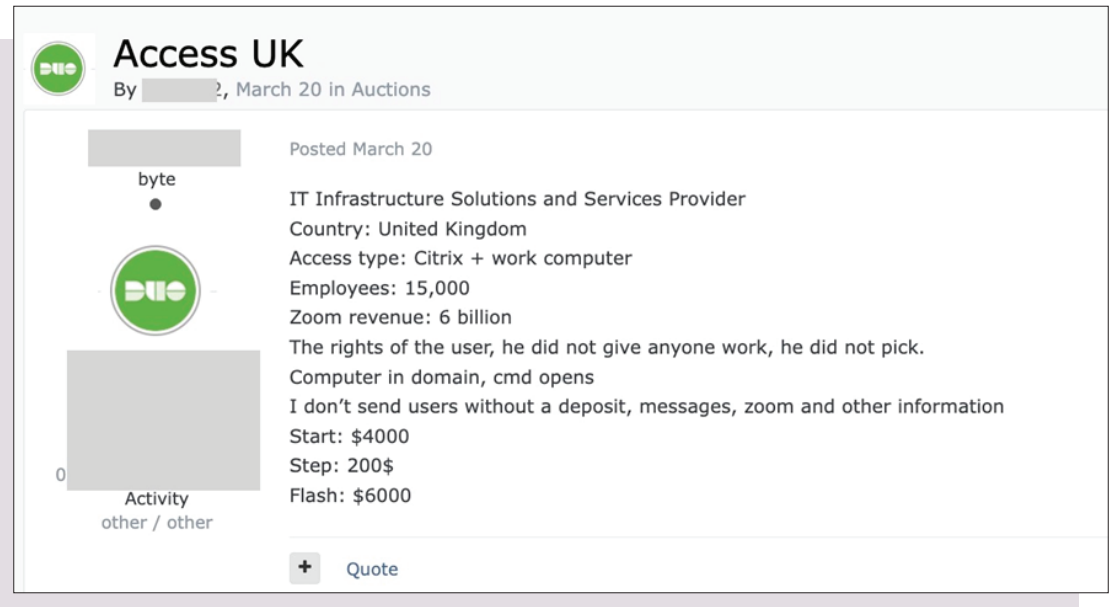
Cyber insurance also likely has a more limited influence on victim selection than some suggest. At any given point, ransomware affiliates may have access to a large number of compromised networks, either through their own efforts or because of the potential to purchase access through cybercriminal brokers and marketplaces. This means that ransomware operators and affiliates may have to prioritise some potential victims over others.

Listings by ransomware operators and initial access brokers on cybercriminal forums and marketplaces give some indication of the information that is used to prioritise potential victims. Advertisements for compromised networks by initial access brokers follow a similar pattern on cybercriminal forums and marketplaces. Typically, these listings include information on:

- Victim country.
- Annual revenue.
- Industry.
- Type of access.
- The number of devices on the network.
- Price.[150]

148. NCSC, 'NCSC Annual Review 2021', 17 November 2021, p. 14.
149. Intel471, 'The Relationship Between Access Brokers and Ransomware Crews Is Growing', 2 June 2022, <https://intel471.com/blog/access-brokers-ransomware-relationship-growing>, accessed 1 August 2022; Smilyanets, 'An Interview With Initial Access Broker Wazawaka'; Insikt Group, 'Initial Access Brokers Are Key to Rise in Ransomware Attacks', *Recorded Future*, 2 August 2022, <https://go.recordedfuture.com/hubfs/reports/cta-2022-0802.pdf>, accessed 29 December 2022.
150. Jim Walter, 'More Evil Markets: How It's Never Been Easier to Buy Initial Access to Compromised Networks', *SentinelOne*, 17 August 2022, <https://www.sentinelone.com/blog/more-evil-markets-how-its-

Figure 3: An Access Broker Advertises a Compromised Organisation Based in the UK



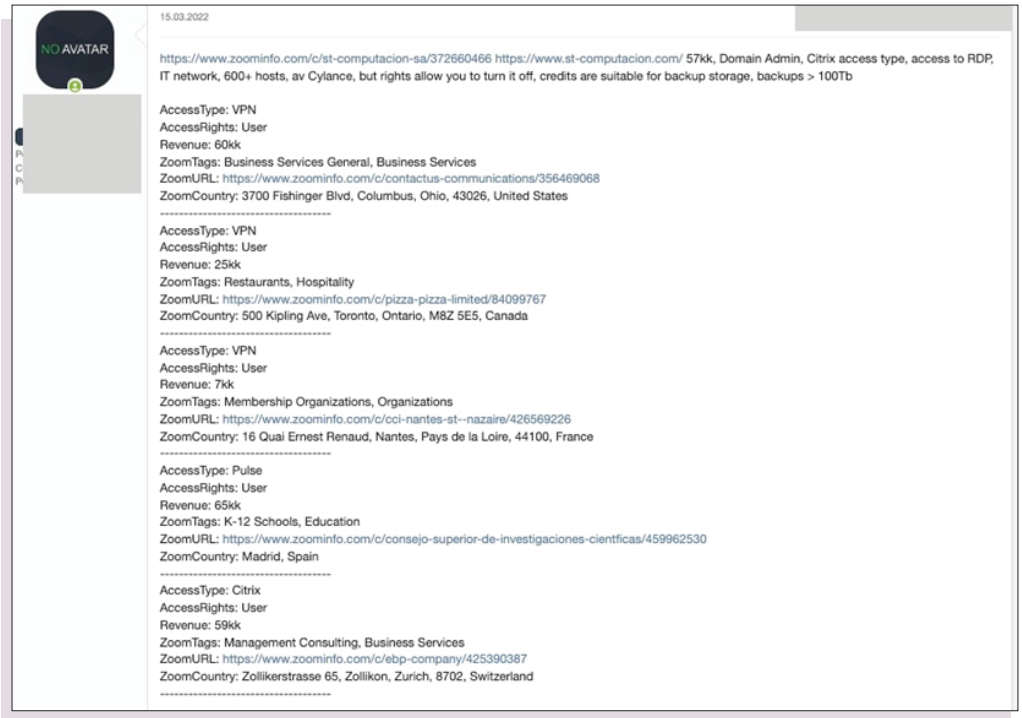
Source: Jim Walter, 'More Evil Markets: How it's Never Been Easier to Buy Initial Access to Compromised Networks', *SentinelOne*, 17 August 2022, <https://www.sentinelone.com/blog/more-evil-markets-how-its-never-been-easier-to-buy-initial-access-to-compromised-networks/>, accessed 29 December 2022.

These advertisements can be developed quickly with open source commercial services such as Zoominfo, which collates this type of information on millions of businesses.[151]

never-been-easier-to-buy-initial-access-to-compromised-networks/>, accessed 29 December 2022; Insikt Group, 'Initial Access Brokers Are Key to Rise in Ransowmare Attacks', p. 3.

151. Brian Krebs, 'Conti Ransomware Group Diaries, Part III: Weaponry', *Kreb's on Security*, 4 March 2022, <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>, accessed 30 December 2022.

Figure 4: An Access Broker Lists Several Compromised Organisations for Sale on a Criminal Marketplace

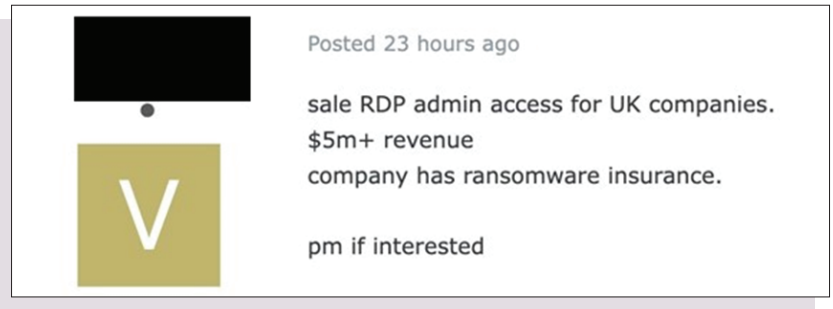


Source: Walter, 'More Evil Markets'.

This indicates that once ransomware affiliates choose to purchase access to specific victims, this is likely based on a range of metrics – especially country, revenue, number of compromised hosts and sector – that does not typically include whether a victim has cyber insurance. Although there is at least one example in open source reporting of an access broker listing which includes information on cyber insurance, this does not appear to be widespread (see Figure 4). Instead, affiliates likely focus on purchasing access to potential victims in specific countries (particularly in the US and Europe); in certain sectors that may be more likely to pay because of the need for continuous operations or because they retain sensitive data; and larger organisations that may be able to pay more lucrative ransoms.[152] It remains the case, however, that potential victims in certain countries[153] or of a certain size[154] may be more likely to have cyber insurance than others.

152. DFIR 1, 24 September 2021; DFIR 5, 1 November 2021; cyber insurance claims 3, 1 December 2021.
153. For instance, in countries where cyber insurance penetration is higher.
154. The UK government's cyber breaches survey, for instance, suggests that uptake of cyber insurance is much higher among larger organisations. See Department for Digital, Culture, Media and Sport, 'Cyber Security Breaches Survey 2022', updated 11 July 2022.

Figure 5: An Access Broker Advertises a Compromised Organisation that Apparently has Cyber Insurance



Source: Harlan Carvey, 'Threat Advisory: Hackers Are Selling Access to MSPs', *Huntress*, 28 July 2022, <https://www.huntress.com/blog/threat-advisory-hackers-are-selling-access-to-msps>, accessed 30 December 2022.

In summary, there is no firm evidence (at least in the public record) to suggest that cybercriminals, ransomware operators and affiliates are regularly adopting tactics to deliberately identify and gain access to organisations with cyber insurance.

Using Cyber Insurance Policies as Leverage in Negotiations

There is more compelling evidence that criminals conducting negotiations are sometimes using stolen cyber insurance policy documents as leverage in negotiations.[155] While this could make it more difficult for insureds and ransomware negotiators to reduce the value of ransom payments, it is not the most significant factor that affects the pricing and negotiation outcome.

Once ransomware affiliates have gained access to an organisation's networks, they will often conduct further internal reconnaissance to understand the target before exfiltrating data and/or deploying the ransomware payload. As part of this process, some affiliates attempt to steal financial information from a victim's network to inform negotiation strategies and set ransom demands. This can be used to complement open source intelligence gathering through commercial business tools such as Zoominfo to identify a victim's annual revenues and profits.

Some ransomware affiliates also steal insurance policy documents as part of this approach. Open source reporting on Conti ransomware, for example,

155. DFIR 1, 24 September 2021; cyber threat intelligence 3, 4 October 2021; DFIR 8, 19 January 2022; ransomware recovery 1, 3 November 2021; cyber insurance claims 3, 1 December 2021; insurance industry association 3, 24 November 2021.

highlights a leaked 2021 training manual in which affiliates were instructed to search for and exfiltrate files related to the following insurance-related keywords:

- Cyber.
- Policy.
- Insurance.
- Endorsement.
- Supplementary.
- Underwriting.
- Terms.[156]

How does this affect ransom discipline? When it does happen, it likely creates a dynamic that would not exist without insurance. At the very least, it makes it much more difficult for negotiators to drive down ransom demands.[157] A study by NCC Group of more than 700 ransomware negotiations between 2019 and 2021 found that the theft of cyber insurance policy documents 'limits the options for any negotiation severely'.[158] It is logical, therefore, to conclude that stolen information on insurance policies contributes to inflated ransoms in some cases. This may be particularly true for smaller organisations because policy limits tend to be much higher than cash reserves.[159]

However, it is also important not to overemphasise the impact of this tactic as an influence on ransomware negotiations and the size of payments. First, it is not clear how common it is for ransomware affiliates to successfully steal insurance policy documents. Second, as highlighted above, ransomware operators and affiliates use a range of open source and stolen financial information on victims to inform negotiations and pricing.[160] Indeed, a victim's annual revenue appears to be the most important metric that helps criminals set ransom demands.[161]

156. GitHub, 'CobaltStrike MANUAL_V2.docx', <https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak/blob/main/CobaltStrike%20MANUAL_V2%20.docx>, accessed 10 August 2022; Lawrence Abrams, 'Conti Ransomware Prioritizes Revenue and Cyberinsurance Data Theft', *Bleeping Computer*, 17 August 2021, <https://www.bleepingcomputer.com/news/security/conti-ransomware-prioritizes-revenue-and-cyberinsurance-data-theft/>, accessed 9 July 2023. That Conti uses this tactic was further reinforced by chat logs in the 2022 Conti leaks. See Check Point, 'Behind the Curtains of the Ransomware Economy – the Victims and the Cyber-Criminals', 28 April 2022, <https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cyber-criminals/>, accessed 12 August 2022.
157. Ransomware recovery 1, 3 November 2021; insurance industry association 3, 24 November 2021.
158. Pepijn Hack and Zang-Yu Wu, '"We Wait, Because We Know You.": Inside the Ransomware Negotiation Economics', NCC Group, 12 November 2021, <https://research.nccgroup.com/2021/11/12/we-wait-because-we-know-you-inside-the-ransomware-negotiation-economics/>, accessed 15 July 2022.
159. Ransomware recovery 1, 3 November 2021.
160. Claims 3, 1 December 2021; DFIR 8, 19 January 2022; Hack and Wu, '"We Wait, Because We Know You."'; Check Point, 'Behind the Curtains of the Ransomware Economy – the Victims and the Cyber-Criminals'.
161. Hack and Wu, '"We Wait, Because We Know You."'; Check Point, 'Behind the Curtains of the Ransomware Economy – the Victims and the Cyber-Criminals'; Vladimir Kropotov et al., 'What Decision-Makers Need to Know About Ransomware Risk', Trend Micro, 23 February 2023.

The Net Effect of Cyber Insurance on Ransom Payments

Taken together, the range of effects cyber insurance has on both victim and attacker decision-making towards ransom payments emphasises the need to avoid falling prey to simple explanations about the relationship between cyber insurance and the ransomware business model. As one senior director at a ransomware recovery firm remarked in the workshop, 'this concept that the insurance carriers are pushing payments or not pushing payments really oversimplifies an intriguing series of events'.[162]

There is no smoking gun uncovered by this research that victims with insurance are much more likely to pay than those without. Although some cyber security practitioners and policymakers argued in interviews that insurers encourage insureds to pay ransoms on the basis of cost–benefit analysis, this does not appear to reflect the reality of the limited involvement insurers have in ransomware response.[163] Most insurers do not advise victims to pay or not pay ransoms and do not authorise payments without at least some due diligence. It is also reasonable to conclude that most organisations with cyber insurance – particularly SMEs – are likely to manage ransomware incidents better than those without, given the access to services, expertise and intelligence.

At the same time, there is also no strong evidence that insurers or the ransomware response services they provide access to are instilling ransom discipline across the market. What constitutes a reasonable 'last resort' for a payment remains ambiguous, and likely varies, given the lack of established best practices around ransomware crisis management and negotiations. This also contributes to the continued challenges that insurers face around reducing the price of ransoms in cases where insureds do choose to pay – particularly given the shift to data exfiltration and double extortion. The discovery and exfiltration of cyber insurance policies by threat actors may also inflate ransom payments if they are used as leverage in negotiations.

Nevertheless, these findings do not necessarily rule out the possibility that insurance incentivised the payment of ransoms at greater scale in the past. Indeed, a theme that bubbled below the surface in some interviews and during the workshop was that insurers were even less willing or able to encourage

162. RUSI workshop, 17 February 2022.
163. Government 2, 1 December 2021; Government 3, 1 December 2021; Government 4, 10 January 2022; Cyber security consultant 1, 24 September 2021; Cyber security consultant 2, 4 October 2021; DFIR 9, 4 February 2022.

ransom discipline when the market was soft, insureds were less prepared, the ransomware response industry was more immature and ransom payments were smaller.[164]

According to a senior director from a ransomware recovery firm who took part in the workshop:

> A few years ago, we were definitely seeing companies paying ransoms not as the last resort. It was ridiculous and outrageous behaviour and I think some of that has coloured a lot of the public's perception of what was going on. What you're seeing at the moment is definitely a last resort however you define it. But there was a wild west, and it smeared some reputational problems that happened out of it.[165]

If the cyber insurance and ransomware response industries are on an evolutionary ransom payment journey, it is worth remembering that this has taken place in the absence of government intervention on ransom payments and minimal advice from security agencies and law enforcement. Indeed, decisions around ransom payments have mostly been left to the private sector,[166] which makes it unsurprising that insurers and victims have often made decisions that prioritise enterprise, business continuity and sometimes even reducing societal harm when essential services or vulnerable groups are at risk over the preferences and priorities of the UK government. This does not mean that the insurance industry should be given a free pass, but rather that it has sometimes been a convenient scapegoat for those seeking to assign blame, in the context of the inability of technology and cyber security companies, governments and law enforcement to make a significant impact on the ransomware business model.

Reducing the Profitability of the Ransomware Business Model Through Insurance

Although there are some signs that the insurance industry is taking steps to stabilise the growth of ransom payments covered by insurance, it can still do much more to instil ransom discipline in the ransomware response ecosystem

164. Underwriter 2, 15 October 2021; cyber insurance underwriter 3, 18 October 2021; cyber insurance claims manager, RUSI workshop, 17 February 2022; senior director at a ransomware recovery firm, RUSI workshop, 17 February 2022.
165. Senior director at a ransomware recovery firm, RUSI workshop, 17 February 2022.
166. Wheeler and Martin, 'Should Ransomware Payments Be Banned?'.

and reduce the profitability of ransomware for criminals.[167] Insurers' role as convenors of ransomware response services gives them considerable power to reward firms that drive best practices around ransom discipline and guide victims towards payment only as a last resort. This potential has yet to be fully tapped. The lack of clearly defined negotiation protocols and the difficulties in learning from incidents have made it difficult to develop a sense of collective responsibility and shared best practices among cyber insurers for ransomware response.[168]

Chapter IV outlines how insurers and governments may overcome some of these challenges and move towards the most realistic positive outcome – market-wide ransom discipline, which would see fewer victims paying ransoms and, when necessary, paying lower demands. This would reduce the profitability of the ransomware business model without criminalising payments and punishing victims.

167. Shortland, Keatinge and MacColl, 'Insurance as Crime Governance'.
168. This may be in part because insurers find it difficult to learn from ransomware incidents and negotiations because potential litigation risks mean external counsels limit the development of formal reports. See Daniel Schwarcz, Josephine Wolff and Daniel Woods, 'How Privilege Undermines Cybersecurity', *Harvard Journal of Law and Technology* (Vol. 36, No. 2, 2023).

III. The Role of Cyber Insurance in Raising Costs for Cybercriminals

Disrupting the ransomware criminal enterprise also involves looking beyond the payment question. This chapter explores how cyber insurance can improve the cyber security and resilience of organisations to make them more difficult targets. This has the potential to negate profit opportunity for criminals and increase the costs of conducting successful ransomware operations. Although the cyber insurance industry has played a frustratingly limited role in reducing the threat from cybercrime in the past, significant losses mean that the market is now sufficiently incentivised to find ways to make it more difficult and more costly for cybercriminals to profit from ransomware.

The research found that successive years of losses from ransomware have led to more stringent security requirements and risk selection by underwriters. Although the overall effect of this on the frequency and severity of ransomware attacks remains to be seen, by linking improvements in security practices to coverage, cyber insurance is currently one of the few market-based levers for incentivising organisations to implement security controls and resilience measures. This is particularly true of SMEs, who are less likely to have well-developed and entrenched cyber security practices or the financial incentive to implement them. However, continued challenges around collecting and assessing reliable cyber risk and forensic claims data continue to place limits on the market's effectiveness as a mechanism for reducing ransomware risk.

Incentivising Better Cyber Security and Resilience Practices Through Insurance

As noted in Chapter I, a key driver of ransomware and other forms of cybercrime is poor cyber security practices and cyber hygiene. Public and private sector organisations of all sizes continue to face commercial and technical barriers to effectively managing the risk from ransomware.

Researchers and policymakers have long speculated about the potential role cyber insurance could play as a lever in improving cyber security. While the primary purpose of insurance is to transfer risk, a byproduct is that it can also improve security and safety in some cases. In the past, other types of insurance have helped reduce economic, physical and technological risk and improved risk management practices for individuals and businesses.[169] The insurance industry has also contributed to efforts to control other forms of crime by hardening targets, improving security measures, and working with governments and law enforcement.[170] However, as a 2021 RUSI paper on cyber insurance highlighted, there is scant empirical evidence that cyber insurance is improving cyber security.[171] In the soft market, insurers were largely unwilling or unable to use carrots or sticks to incentivise organisations to invest in better risk management.

However, our research highlights that there have been significant changes between 2020 and 2021. The hard market and losses arising from ransomware have transformed risk selection. Interviewees highlighted that the market's risk appetite is now much more closely correlated to underwriters' assessments of organisations' cyber maturity and security controls.[172] While some insurers have stepped back from cyber insurance, other have pursued innovations in services and investment in technical expertise and tools. Even so, progress is still uneven and varies significantly by insurer. Moreover, continued challenges around collecting and analysing cyber risk data limit the market's ability to accurately assess organisations' risk and standardise and implement best practices more effectively.

Mechanisms for Incentivising Organisations to Mitigate Ransomware Risk

Through interview analysis, we identified four mechanisms through which cyber insurance can incentivise organisations to mitigate some of their risk from ransomware by improving cyber security and resilience practices.

169. See MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 9.
170. Shortland, Keatinge and MacColl, 'Insurance as Crime Governance'.
171. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'.
172. This point was emphasised by all 10 cyber insurance underwriters and all five cyber insurance brokers interviewed for the research.

Assessing Ransomware Risk and Security Practices

First, by assessing a potential policyholder's risk profile, insurers can identify potential risks, poor cyber hygiene and bad practices that ransomware operators can exploit. Typically, this is done via an initial risk assessment that includes a combination of questionnaires and – in many cases – an external network scan of an organisation's IT infrastructure. This information can be combined with claims and loss data and, sometimes, cyber threat intelligence on ransomware trends.[173]

Questionnaires query a range of business, IT and security information. Their length varies depending on the size of an organisation, and large businesses are asked considerably more questions than SMEs.[174] In general, insurers and businesses highlighted that questionnaires have become much longer, more granular and more focused on assessing technical security controls since early 2021. As one chief risk officer at a technology company noted, 'the questions are very specific, and they're the sort of questions you don't want to be asked if you're a big company'.[175] In some cases, questionnaires are also more closely aligned with existing best practice cyber security frameworks such as NIST than in the past,[176] but it is not clear how widespread this is.

Organisations must now also complete a supplemental ransomware questionnaire to obtain ransomware coverage. This involves answering dedicated questions about security controls and business continuity practices that underwriters believe mitigate some of the risk from ransomware. Crucially, organisations of all sizes must fill out these supplemental applications.[177] This represents a significant change from the soft market approach, when smaller organisations could obtain ransomware coverage on the basis of very limited proposal forms.[178]

Insurers also use external scans to identify vulnerabilities and poor cyber hygiene on internet-facing IT infrastructure. Some insurers have developed or

173. Several insurers highlighted that they have developed in-house threat intelligence teams and/or purchase access to threat intelligence feeds from specialist vendors. Underwriter 2, 15 October 2021; cyber insurance executive 1, 11 October 2021; cyber insurance claims 1, 24 September 2021.
174. Underwriter 9, 1 December 2021.
175. Technology 1, 10 November 2021.
176. Underwriter 1, 13 October 2021; defence 1, 16 November 2021.
177. Gallagher, 'Cyber and Data Insurance Market Overview, Update and Risk Management Standards', 27 April 2022, <https://www.ajg.com/uk/-/media/files/gallagher/uk/news-and-insights/cyber-and-data-insurance-market-update-2022.pdf>, accessed 10 August 2022; Howden, 'Cyber Insurance: A Hard Reset 2.0'; SwissRe, 'Cyber Insurance: Strengthening Resilience for the Digital Transformation', November 2022, p. 18.
178. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 13; Nurse et al., 'The Data That Drives Cyber Insurance', p. 3.

acquired their own in-house scanning capabilities,[179] while others rely on third-party providers. Although external scans are prone to producing false positives and are not by themselves indicative of an organisation's overall risk profile,[180] they can be useful because they mirror the approach taken by ransomware operators and initial access brokers,[181] who scan for internet-facing vulnerabilities and open or poorly secured RDP ports to gain access to victims. As one incident response practitioner summarised, 'It's not like you can take one of these tools, look at somebody's network and say "yes, this is how secure they are", I don't believe it works that well. But for some immediate, urgent things you need to fix, it does make a difference'.[182] At best, they are a means of highlighting low-hanging fruit that ransomware operators might exploit. At worst, an overreliance on them could reduce the credibility of insurers with purchasing organisations and cyber security practitioners.[183]

As with scans, there are limitations to insurers' approaches to questionnaires. Brokers and chief information security officers, in particular, suggested that questions around security controls are often too binary and fail to capture the nuance of cyber risk. As one director at a cyber risk management and brokerage firm highlighted, 'A lot of the phraseology of the questions suggest a closed or fairly binary answer. "Have you got MFA [multi-factor authentication]?" It isn't a yes or no answer. It's a "yes, but", or "we have this deployed" or "we use MFA at our VPN level before you get access to our system" so, there is more context that's needed'.[184] There are also some doubts about the ability of insurers to interpret answers in questionnaires, given the limited technical cyber security expertise in the underwriting community.[185] A final concern is whether insurers can validate answers to some questions given they cannot, at least for now, access internal telemetry or verify configurations of some controls or security tools. While these concerns are valid, they are more applicable to larger and more mature organisations with complicated IT estates. On balance, the shift to more detailed risk assessments is a positive step forward, even if many insurers' approaches require improvements.

179. Underwriter 2, 15 October 2021; cyber insurance underwriter 9, 1 December 2021; cyber insurance underwriter 8, 12 November 2021; cyber insurance executive 1, 11 October 2021.
180. DFIR 4, 27 October 2021.
181. Underwriter 5, 1 November 2021; cyber risk management services 1, 29 October 2021; cyber risk analytics 2, 28 October 2021; cyber security consultant 2, 4 October 2021; DFIR 4, 27 October 2021; CTI 2, 24 September 2021.
182. DFIR 4, 27 October 2021.
183. DFIR 2, 7 October 2021; cyber security consultant 2, 4 October 2021; cyber risk analytics 2, 28 October 2021.
184. Cyber risk management services 1, 29 October 2021.
185. DFIR 2, 7 October 2021; cyber insurance broker 2, 18 November 2021; DFIR 9, 4 February 2022.

Linking Security Practices to Ransomware Coverage, Limits and Terms

> If you don't have the 10 key things that we now know will stop 80–90% of ransomware, you don't get insurance, or you get a much smaller amount, and it's a lot more expensive, and your deductible is higher.[186]

Arguably the most significant lever insurers currently have is that some security controls are now a prerequisite for obtaining coverage or acceptable limits for ransomware coverage. This provides an incentive for organisations to introduce cyber security and resilience measures if they want to transfer their residual risk from ransomware and other forms of cybercrime. This marks a significant change from market conditions before 2021.[187]

During interviews, multiple underwriters and brokers recited similar lists of security controls that the market requires. Although insurers are not yet following standardised requirements, there are commonalities. Common controls include: endpoint detection and response (EDR) solutions, remote access controls, regular patching cadences, and email filtering and authentication methods. Some insurers are also requiring that organisations remediate vulnerabilities with known exploits or open RDP ports identified by external network scans before they will offer terms or coverage.[188] One underwriter at a specialist cyber insurer highlighted that 'if we're looking at a new buyer and we identify that they have an open RDP port, we're going to decline that risk outright. They close the port, we verify it, we go ahead and offer terms'.[189]

Perhaps most significant, however, is the emphasis on requirements around MFA – either across all accounts or for remote access accounts/services – and regularly updated off-site backups. Indeed, MFA and off-site backups now appear to be a prerequisite for nearly all organisations to obtain ransomware coverage,[190] with the exception of micro businesses and some small businesses in lower-risk sectors.[191] 'Companies that don't have MFA for remote access are finding it really

186. Underwriter 4, 21 October 2021.
187. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 18; Woods and Moore, 'Does Insurance Have a Future in Governing Cyber Security?'.
188. Underwriter 9, 1 December 2021; cyber insurance underwriter 8, 12 November 2021; cyber insurance underwriter 4, 21 October 2021.
189. Underwriter 9, 1 December 2021.
190. Broker 1, 12 November 2021; cyber risk management services 1, 29 October 2021; cyber insurance broker 3, 1 December 2021; cyber insurance underwriter 2, 15 October 2021; cyber insurance underwriter 9, 1 December 2021; cyber insurance underwriter 4, 21 October 2021; cyber insurance underwriter 7, 2 November 2021.
191. Some interviewees in the UK market indicated that micro and some small businesses can obtain coverage without MFA (cyber insurance executive 1, 11 October 2021; cyber insurance underwriter 10, 10 December 2021). For market reporting, see Gallagher, 'Cyber and Data Insurance Market Overview, Update and Risk Management Standards'.

hard to get coverage', highlighted one cyber insurance executive, 'and that's driven much broader adoption of MFA'.[192] This sentiment was echoed by a broker, who explained that MFA 'is almost the price of admission to get an insurance policy, with very rare exceptions'.[193]

In the current market, this means that an organisation's cyber risk management is now much more closely tied to its insurability. Interviewees emphasised that organisations that do not meet insurers' minimum security standards will not be able to obtain ransomware coverage or coverage full stop,[194] or that any ransomware coverage they do get will be heavily sub-limited.[195] This also means that some insurers are either turning potential policyholders away or not renewing existing clients.[196]

There are also some signs that insurers are starting to use contractual obligations to incentivise better cyber security.[197] In effect, this means that claims payments can be conditional on the implementation of security controls or remediation of known vulnerabilities. In August 2022, for instance, the insurer Travelers asked a court to void a US-based insured's cyber policy because it had misrepresented its use of MFA, and then been compromised by ransomware.[198] Another example is the 'neglected software vulnerabilities' extension that Chubb has now included in its cyber policies. In the simplest terms, this means that policyholders that do not patch software vulnerabilities within a certain time period will assume more of the risk and financial cost that results from a claim.[199] However, the extent to which the market as a whole will move towards this kind of approach is uncertain. Several insurers highlighted that they would prefer to prioritise maintaining relationships with clients and building market share.[200]

192. Cyber insurance executive 1, 11 October 2021.
193. Broker 1, 12 November 2021.
194. Claims 1, 24 September 2021; cyber insurance broker 2, 18 November 2021; cyber insurance underwriter 2, 15 October 2021; cyber insurance underwriter 4, 21 October 2021; cyber insurance underwriter 5, 1 November 2021; cyber security consultant 2, 4 October 2021; DFIR 6, 23 November 2021; cyber insurance cyber insurance broker 1, 12 November 2021; insurance lawyer 1, 28 October 2021; cyber insurance executive 1, 11 October 2021; cyber risk management services 1, 29 October 2021; cyber risk management services 2, 30 November 2021; Howden, 'Cyber Insurance', p. 37.
195. Broker 1, 12 November 2021; cyber insurance underwriter 1, 13 October 2021.
196. Underwriter 2, 15 October 2021; cyber insurance underwriter 5, 1 November 2021.
197. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 18; Woods and Moore, 'Does Insurance Have a Future in Governing Cyber Security?'.
198. Chad Hemenway, 'Travelers, Policyholder Agree to Void Current Cyber Policy', *Insurance Journal*, 30 August 2022, <https://www.insurancejournal.com/news/national/2022/08/30/682564.htm>, accessed 4 September 2022.
199. Chubb, 'Chubb Address Growing Cyber Risks With a Flexible and Sustainable Approach', 13 October 2021, <https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/cyber-enterprise-risk-management-cyber-erm/documents/pdf/2021-10.13_v3_17-01-0295_Widespread_Events_Endorsements.pdf>, accessed 20 February 2023.
200. Claims 1, 29 September 2021; cyber insurance underwriter 9, 1 December 2021; cyber insurance underwriter 8, 12 November 2021; cyber insurance executive 1, 11 October 2021.

Providing Roadmaps to Insurability

> Clients understand they need to do this. It's a rare case now where they are completely ignorant of cyber risk and do not understand what they should be doing to at least mitigate it. In past years, they've been able to insure this and the insurance hasn't been terribly expensive, so it's been easy to put off. That is not the case anymore … [cyber insurance] has proved to be a real catalyst to get companies to do this.[201]

If linking an organisation's risk from ransomware to insurability is incentivising organisations to implement security controls, what happens next? Interviews highlighted that the insurance industry is increasingly providing advice or risk management consulting to organisations that are deemed too high risk to obtain a policy or ransomware coverage.

Arguably more significant, however, is the role that insurance brokerages play. Due to the hard market and tighter underwriting requirements, brokers are more rigorously pre-screening clients' cyber maturity before going to market. Brokers have access to multiple questionnaires, meaning they can aggregate the minimum security controls that are a prerequisite for a policy in most cases.[202] Some brokerages have developed their own ransomware readiness checklists which clients must fill out to assess their likelihood of obtaining ransomware coverage.[203] Because brokers work on commission, they are financially incentivised to ensure clients meet security requirements in tough market conditions.

Large brokerages are also increasingly providing cyber risk management consulting and services. Several have acquired specialist cyber security or consulting firms,[204] or developed their own in-house teams of cyber security practitioners.[205] This diversification allows them to generate revenue from new services, but also to provide cyber security expertise to organisations seeking to obtain cyber insurance and ransomware coverage.[206] Some examples of what

201. Broker 1, 12 November 2021.
202. Broker 1, 12 November 2021; cyber risk management services 1, 29 October 2021; cyber risk management services 2, 30 November 2021; cyber insurance broker 3, 1 December 2021; cyber insurance broker 5, 8 December 2021.
203. Cyber risk management services 1, 29 October 2021; cyber risk management services 2, 30 November 2021; cyber insurance broker 5, 8 December 2021.
204. Slipcase, 'Aon Acquires Cytelligence, a Leading International Cyber Security Firm With Deep Expertise in Cyber Incident Response and Digital Forensic Investigations', <https://www.slipcase.com/view/aon-acquires-cytelligence-a-leading-international-cyber-security-firm-with-deep-expertise-in-cyber-incident-response-and-digital-forensic-investigations>, accessed 20 February 2023; Alex Clere, 'Gallagher Buys Crisis & Security Consultancy AnotherDay', InsurTech, 9 August 2022, <https://insurtechdigital.com/articles/gallagher-to-buy-crisis-and-security-consultancy-anotherday>, accessed 20 February 2023.
205. Broker 3, 1 December 2021.
206. Marsh, 'Ransomware', <https://www.marsh.com/us/services/cyber-risk/products/ransomware.html>, accessed 8 July 2023; Aon, 'Ransomware Defence', <https://www.aon.com/ransomware-defence-emea.aspx>, accessed 8 July 2023; WTW, 'Cyber Risk Management', <https://www.wtwco.com/en-GB/Solutions/

this means in practice apparently include helping smaller clients gain Cyber Essentials certification, running penetration tests, and providing guidance and practical assistance around implementing MFA.[207] These types of activities are particularly useful for SMEs, but are of limited value to more mature organisations.

In some cases, if an organisation is unable to obtain coverage because of their risk posture, underwriters or risk engineers may also directly identify which controls need to be implemented.[208] 'Customers are now starting to go away and implement some of these controls', explained one underwriter, 'and then they come back in 2–3 months' time, and then they're able to get a cyber insurance policy'.[209] In other cases, underwriters will insert subjectivities into contracts which make coverage conditional on recommended security controls – particularly MFA – being implemented within 30 or 60 days of the start of the policy period.[210]

Access to Pre-Breach Services

Finally, many cyber insurers provide so-called 'pre-breach' services which seek to prevent incidents. This has become an integral part of the service offering for some insurers. Perhaps more than any other aspect of cyber insurance, pre-breach services demonstrate the widening gap between traditional carriers and specialist cyber insurers that are more security focused. Although most of these services are not specific to ransomware, they have the potential to provide additional expertise, training and tools to insureds.[211] However, as noted in a previous RUSI paper, insurers have faced considerable challenges around incentivising insureds to use pre-breach services and making them sufficiently actionable and user friendly.[212]

The most significant development over the last couple of years is the development and dissemination of threat intelligence. Specialist cyber insurers are increasingly building or acquiring their own in-house threat intelligence teams to identify potential threats to insureds.[213] When coupled with regular external scans, this approach can identify known vulnerabilities on insureds' internet-facing

cyber-risk-management>, accessed 5 July 2023 ; Silverfort, 'Howden Group Simplifies Cybersecurity Insurance Compliance With Silverfort's Unified Identity Protection', 12 December 2022, <https://www.silverfort.com/press-news/news/howden-group-simplifies-cybersecurity-insurance-compliance-with-silverfort/>, accessed 5 July 2023.

207. Broker 3, 1 December 2021.
208. Underwriter 1, 13 October 2021; cyber insurance underwriter 4, 21 October 2021; cyber insurance underwriter 7, 2 November 2021.
209. Underwriter 1, 13 October 2021.
210. Cyber risk management services 1, 29 October 2021; cyber insurance claims 1, 29 September 2021; cyber insurance underwriter 2, 15 October 2021; cyber insurance underwriter 4, 14 October 2021.
211. For examples of the range of services offered by insurers, see MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', pp. 21–23.
212. See *ibid*.
213. Claims 1; cyber insurance underwriter 7; cyber insurance underwriter 2; cyber insurance executive 1.

infrastructure that ransomware operators are known to exploit. Examples of this include identifying Log4J,[214] Log4Shell[215] and a variety of vulnerabilities in Microsoft Exchange servers.[216] These vulnerabilities have all been exploited by ransomware operators.[217] Because some insurers recognise that this intelligence is of little use to some insureds if it is not actionable, they are also providing direct remediation advice through phone calls with in-house security consultants, bespoke mobile apps or advisories.[218]

As some cyber insurers in the SME market have books that number in the tens of thousands of insureds,[219] they can push out threat intelligence and advice on remediation at scale to smaller organisations that are less likely to have access to these services without insurance. One underwriter provided a specific example of how his company was able to help identify and remediate a critical Microsoft Exchange vulnerability in 2021: 'we were able to scan our entire book immediately as soon as that hit and find out how many of our clients had that vulnerability, and then we were on the phone, on the emails, getting them to remediate. So, we narrowed that down from 750 companies in our book that had that vulnerability to five or six within a matter of a couple of weeks'.[220] At least one specialist cyber insurer is going even further and identifying active malware or tooling on

214. At-Bay, 'Log4j Vulnerability Discovery Tool', 15 December 2021, <https://www.at-bay.com/articles/log4j-checker/>, accessed 8 July 2023; Tiago Henriques, 'New Vulnerability in Log4j – CVE-2021-44228', 18 November 2021, <https://www.coalitioninc.com/blog/new-vulnerability-in-log4j-cve-2021-44228>, accessed 8 July 2023; Corvus, 'Available Now: Log4j Vulnerability Discovery With Tools From Corvus and Crowdstrike', 12 January 2022, <https://www.corvusinsurance.com/news/log4j-scan-tool>, accessed 8 July 2023.
215. CFC Underwriting, 'Client Advisory: Log4Shell Vulnerability', 13 December 2021, <https://www.cfcunderwriting.com/en-gb/resources/advisories/2021/12/log4shell/>, accessed 8 July 2023.
216. CFC Underwriting, 'Remediation Guidance: ProxyLogon Vulnerability', March 2021, <https://www.cfcunderwriting.com/media/3765/proxylogon-remediation-guidance-cfc-march-21.pdf>, accessed 8 July 2023; CFC Underwriting, 'Client Advisory: ProxyShell Vulnerability Remediation', 26 August 2021, <https://www.cfcunderwriting.com/en-gb/resources/advisories/2021/08/client-advisory-proxyshell-vulnerability-remediation/>, accessed 8 July 2023; Corvus, 'Microsoft Exchange Vulnerability Advisory', 4 October 2022, <https://help.corvusinsurance.com/microsoft-exchange-vulnerability-advisory-september-2022>, accessed 8 July 2023.
217. Liam Tung, 'Ransomware: Hackers Are Using Log4j Flaw as Part of Their Attacks, Warns Microsoft', *ZDNET*, 11 January 2022, <https://www.zdnet.com/article/ransomware-warning-hackers-are-using-log4j-flaw-as-part-of-their-attacks-warns-microsoft/>, accessed 8 July 2023; Sean Gallagher and Peter Mackenzie, 'Conti Affiliates Use ProxyShell Exchange Exploit in Ransomware Attacks', *Sophos News*, 3 September 2021, <https://news.sophos.com/en-us/2021/09/03/conti-affiliates-use-proxyshell-exchange-exploit-in-ransomware-attacks/>, accessed 8 July 2023; Tyler McLellan, Joshua Shilko and Shambavi Sadayappan, '(Ex)Change of Pace: UNC2596 Obvserved Leveraging Vulnerabilities to Deploy Cuba Ransomware', 23 February 2022, <https://www.mandiant.com/resources/blog/unc2596-cuba-ransomware>, accessed 8 July 2023.
218. Underwriter 7, 2 November 2021; cyber insurance underwriter 8, 12 November 2021; cyber insurance underwriter 9, 1 December 2021; cyber insurance claims 1, 29 September 2021; cyber insurance claims 2, 11 October 2021.
219. Cyber insurance executive 1, 11 October 2021; cyber insurance underwriter 7, 2 November 2021.
220. Underwriter 8, 12 November 2021.

insureds' networks before ransomware operators encrypt or exfiltrate data.[221] However, it is worth emphasising that these approaches are likely not indicative of the market overall.

Despite this, by and large, insurers continue to face barriers to uptake of pre-breach services. Some interviewees pointed to the challenge of actually connecting the services with IT or security staff, particularly given the fact that many companies will rely on outsourced managed service providers (MSPs).[222] Uptake of services or acting on threat intelligence is also not, for the most part, linked to contractual obligations or coverage.[223] However, several insurers did suggest that if a policyholder repeatedly ignores critical vulnerabilities or open RDP ports identified by scanning during the policy period, they would not renew the policy.[224]

The Perennial Challenge: The Data Gap

> Data is the biggest problem the market has.[225]

Despite continued challenges around uptake of pre-breach services, the cyber insurance market is now a much better mechanism for nudging organisations towards implementing cyber security and resilience measures than it was before 2021. However, a burning question remains: do these measures meaningfully reduce the risk from ransomware?

This is an empirical question that does not currently have a definite answer. Insurers' minimum security requirements for ransomware coverage seem to broadly align with best practice guidance from the UK and US governments on mitigating the threat from ransomware. This is particularly true of offline backups, MFA and hardening remote access services.[226] Indeed, insurers' strong focus on MFA mirrors the current drive by the US Cybersecurity and Infrastructure Security Agency (CISA) to encourage MFA adoption among US organisations.[227]

At the same time, interviewees and workshop participants highlighted the lack of consensus and certainty about which controls (and how they are implemented)

221. CFC Underwriting, 'Cobalt Strike Infection', 19 August 2022, <https://www.cfcunderwriting.com/en-gb/resources/case-studies/incident-prevention/cobalt-strike-infection/>, accessed 15 September 2022.
222. Broker 1, 12 November 2021; insurance industry association 3, 24 November 2021.
223. Claims 3, 1 December 2021; cyber insurance executive 1, 11 October 2021; cyber insurance claims 1, 29 September 2021; cyber insurance underwriter 7, 2 November 2021.
224. Claims 3, 1 December 2021; cyber insurance underwriter 7, 2 November 2021.
225. Broker 2, 18 November 2021.
226. NCSC, 'Mitigating Malware and Ransomware Attacks', 9 September 2021, <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>, accessed 8 July 2023; CISA, 'Stop Ransomware: Bad Practices', <https://www.cisa.gov/stopransomware/bad-practices>, accessed 8 July 2023.
227. CISA, 'Multifactor Authentication', <https://www.cisa.gov/mfa>, accessed 8 July 2023.

reduce the frequency and severity of ransomware. One executive at a specialist insurer, for instance, argued that 'our data does not categorically show that MFA makes that big a difference'.[228]

The difficulty insurers face in establishing with certainty that specific security controls reduce the risk from ransomware points to an ongoing challenge for cyber insurance – namely, the lack of reliable cyber risk and claims data. There are several factors that contribute to this data gap:

- **The underwriting–claims feedback loop**. Some insurers struggle to extract meaningful lessons from claims. By and large, claims teams focus on business and financial data, and are either unwilling or unable to collect technical information from written forensic reports that can then be fed back into underwriting. Instead, they largely rely on more informal feedback.[229] There are several reasons for this. First, it is expensive to conduct thorough forensic reports and may not always be cost effective for insurers in the SME market.[230] Second, forensic investigators are sometimes unable to identify root causes of ransomware attacks or other incidents. Third, lawyers involved in the incident response process may block access to forensic reports to mitigate litigation risk. One recent US-focused study found that 'lawyers routinely limit the information from forensic firms' and that claims teams must largely rely on informal phone calls.[231] Several US interviewees confirmed this as a challenge,[232] although it is unclear if this is also true of less litigious countries like the UK. Taken together, the limitations of the current underwriting–claims feedback loop make it more difficult to identify the most effective loss prevention measures. This is one of the drivers of the trend towards insurers developing their own in-house incident response functions that was highlighted in Chapter II.
- **Dynamic cybercriminal threats**. Insurers' data must account for the fact that threat actors are constantly developing new tactics to bypass defensive measures.[233] The constant evolution of ransomware initial access and monetisation tactics and techniques over the past few years is a good example of how dynamic cyber threats can be (See Chapter I).

228. RUSI workshop, 17 February 2022.
229. As explained by cyber insurance broker 2, cyber insurance executive 1, Corvus cyber insurance underwriter, DFIR 6; Schwarcz, Wolff and Woods, 'How Privilege Undermines Cybersecurity'.
230. Cyber insurance executive 1, 11 October 2021; cyber insurance claims 2, 11 October 2021.
231. Schwarcz, Wolff and Woods, 'How Privilege Undermines Cybersecurity', p. 41.
232. Underwriter 9, 1 December 2021; cyber insurance claims 3, 1 December 2021.
233. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 31; Erin Kenneally, 'Hiding in Plain Sight: Towards Now-Gen Cyber Risk Underwriting', Guidewire, September 2021, <https://www.the-digital-insurer.com/wp-content/uploads/securepdfs/2021/09/1834-GuidewireCyenceRiskHidingInPlainSight.pdf>, accessed 30 August 2022.

- **Static assessments and underwriting**. Underwriting remains largely static and rooted in annual assessments. Although, as highlighted earlier in this chapter, some insurers are conducting external scans on a more regular basis, this is not yet tied to dynamic coverage or pricing. Moreover, external scanning tools are not able to verify the configuration of many security controls.

Raising Costs for Ransomware Operators by Incentivising Cyber Security and Resilience

In summary, there are some signs that cyber insurance is helping to mitigate some of the threat from ransomware by incentivising organisations to improve their cyber security and resilience. However, the effects of cyber insurance on societal cyber security and resilience are unlikely to be experienced equally by all types of organisations. By linking the availability of coverage to minimum security requirements, cyber insurance is likely to have the most impact on organisations with lower baseline levels of cyber security, such as SMEs, or in sectors that have relied on cyber insurance as a crutch in the past. Similarly, pre-breach cyber security services provided by insurers are more likely to fill gaps in capabilities for SMEs than for larger organisations. By contrast, organisations with higher pre-existing levels of cyber maturity may already have many of the minimum security requirements insurers ask for in place, or require more complex approaches to cyber risk management that underwriters with limited technical expertise may struggle to adequately assess.

Although there are reasons for optimism, the cyber insurance market continues to face significant challenges that place limits on its effectiveness as a mechanism for reducing the risk from ransomware and other cyber threats. Most significantly, there are legitimate questions about the reliability of the evidence base that insurers have for assessing the effectiveness of security controls and pricing risk adequately. This is a foundational challenge for cyber insurance. As noted in Chapter I, the low penetration of cyber insurance also places limits on the market's ability to bring positive change at scale.

IV. The Role of Cyber Insurance in Supporting Governmental and Law Enforcement Interventions Against Ransomware

Disrupting the ransomware criminal enterprise must go beyond resilience-building measures and increase the risks for ransomware operators through government and law enforcement activity. This chapter explores the potential role of cyber insurance in supporting UK government and law enforcement initiatives to combat ransomware.

The areas where cyber insurance has the potential to have the most impact on broader efforts to combat ransomware are driving reporting of ransomware attacks and payments, sharing aggregated claims data, and distributing NCSC guidance and intelligence to organisations. However, its current role is restricted by the weakness of existing reporting mechanisms and incentives for both insurers and insureds, along with the lack of meaningful strategic and operational public–private partnerships between the UK government and the insurance industry. The latter reflects both the lack of a perceived rationale for cyber insurers to support UK government initiatives, and the limitations of existing UK government outreach to the market.

Supporting Government and Law Enforcement Interventions

Although progress against ransomware by governments and law enforcement has been frustrating, there has been a steady uptick of successful law enforcement

and offensive cyber operations since 2021.[234] One recent prominent example was the successful infiltration and takedown of the Hive ransomware operation's infrastructure, which allowed law enforcement to distribute more than 300 decryption keys to victims.[235] As highlighted in Chapter I, disruption of ransomware operations may be creating distrust within the ransomware ecosystem, although the overall effect on the frequency and severity of attacks remains to be seen.

However, the ability of governments and law enforcement to both disrupt ransomware operators and support victims is limited by the 'whack-a-mole' nature of operations against Russian organised cybercrime, as well as by a lack of intelligence on cybercriminals and data on the nature and scale of the threat ransomware poses. Designing and resourcing effective responses to ransomware also requires sufficient data on ransomware operators and the impact on victims and the UK as a whole. Ultimately, the perception of the scale and nature of the threat influences the prioritisation of ransomware by governments and law enforcement.

More broadly, law enforcement and cyber security agencies struggle to make connections with victims both during and after ransomware attacks.[236] This means organisations are unable to benefit from lessons generated by victims' experiences with ransomware.

Driving Reporting of Attacks and Ransom Payments

> The only thing that we're particularly confident on is that there's enormous underreporting and we don't really know the scale.[237]

The limitations of existing government data and intelligence on ransomware make increasing reporting of ransomware incidents essential. However, reporting remains frustratingly limited in the UK and other countries. The UK National Crime Agency (NCA), for instance, has estimated that less than 10% of victims report ransomware attacks to UK law enforcement.[238] Challenges around reporting were also highlighted during the operation against Hive, when the FBI revealed

234. Julian-Ferdinand Vögele, 'Ransomware Enforcement Operations in 2020 and 2021', Recorded Future, 31 March 2022, <https://www.recordedfuture.com/ransomware-enforcement-operations-in-2020-and-2021>, accessed 21 September 2022.
235. US Department of Justice, 'US Department of Justice Disrupts Hive Ransomware Variant'.
236. Eleanor Fairford, 'Why More Transparency Around Cyber Attacks is a Good Thing for Everyone', NCSC, 11 May 2023, <https://www.ncsc.gov.uk/blog-post/why-more-transparency-around-cyber-attacks-is-a-good-thing-for-everyone>, accessed 8 July 2023.
237. Government 3, 1 December 2021.
238. Joint Select Committee on National Security Strategy, 'Written Evidence by His Majesty's Government', RAN0018, 30 January 2023, <https://committees.parliament.uk/writtenevidence/114408/pdf/>, accessed 8 July 2023.

that only 20% of victims had reported to law enforcement.[239] This figure was likely inflated as the FBI and other law enforcement agencies proactively contacted victims. There are also no reliable estimates of the number of victims that opt to pay ransoms, nor are there comprehensive law enforcement or regulatory mechanisms for tracking payments.

Cyber insurers could play a role in increasing reporting of ransomware incidents and ransom payments. In many other forms of insurance that cover losses from crime, reporting to law enforcement is required to make a claim. However, in practice, few cyber insurers have mechanisms that incentivise or oblige policyholders to report. We found two examples of UK insurers that require victims to notify law enforcement before a ransom payment is authorised in the interviews for this research, but this appears to be the exception rather than the rule.[240] Some interviewees suggested that victims with insurance are more likely to notify law enforcement or the NCSC because the incident response process is more formalised and well managed,[241] but it is ultimately left to the policyholder's discretion.

This must be seen in the context of the limitations of existing regulatory and law enforcement reporting mechanisms, which are not victim friendly nor well suited to capturing data about ransomware attacks. In the UK, the Information Commissioner's Office (ICO) can wield sticks to drive reporting of ransomware attacks that affect the confidentiality of data, but is not focused on capturing threat or payment-focused data. Law enforcement, for its part, cannot compel or encourage reporting to Action Fraud,[242] and is not tasked or resourced to understand the impact of ransomware on organisations.[243] There are also practical challenges for victims reporting to Action Fraud, as there is no dedicated category for ransomware. More generally, victims are not incentivised to be transparent given commercial, regulatory and reputational considerations.

Finally, there may also be a misperception among victims about the intentions of law enforcement and government agencies, along with a reasonable scepticism

239. Christopher Wray, 'Remarks at Press Conference Announcing the Disruption of the Hive Ransomware Group', FBI, 26 January 2023, <https://www.fbi.gov/news/speeches/director-christopher-wrays-remarks-at-press-conference-announcing-the-disruption-of-the-hive-ransomware-group>, accessed 30 January 2023.
240. Aviva, 'Your Cyber Policy', p. 18, <https://connect.avivab2b.co.uk/brokerPublicProductDocuments/BCOAG15628?productCode=CYB>, accessed 8 July 2023; Hiscox, 'Cyber and Data Insurance: Policy Wording', p. 12, <https://www.hiscox.co.uk/sites/uk/files/documents/2019-03/19029-CyberClear-policy-wording.pdf>, accessed 8 July 2023.
241. DFIR 5, 1 November 2021; insurance industry association 1, 29 October 2021.
242. Action Fraud is the UK's national centre for reporting fraud and cybercrime.
243. Joint Select Committee on National Security Strategy, 'Written Evidence Submitted by RUSI Cyber and the Centre for Financial Crime and Security Studies to the Joint Committee on National Security Strategy's Ransomware Inquiry', RAN0032, 30 January 2023, <https://committees.parliament.uk/writtenevidence/114435/pdf/>, accessed 31 May 2023.

about their willingness and ability to provide support. Interviewees involved in ransomware response, for instance, highlighted that some victims sometimes believe that law enforcement will seek to seize servers or computers for investigations, or ask unwanted questions that are perceived to slow down decision-making or their ability to recover.[244]

Insurers also have legitimate questions around how incentivising reporting of ransomware and other forms of cybercrime to the NCSC and law enforcement directly helps the cyber insurance market. The UK government – and other governments – have not made a compelling carrot- or stick-based argument on why insurers should use levers to encourage reporting, instead relying on appealing to their general sense of altruism. While insurers will ultimately benefit, albeit indirectly, if governments are able to generate more accurate and actionable data on ransomware, this needs to be sold to the industry in a more convincing way.

Strategic and Operational Partnerships With Law Enforcement, Cyber Security Agencies and Government

Beyond reporting, insurers can support broader government initiatives against ransomware by informing the development of policy towards ransomware, sharing aggregated claims data and distributing intelligence more widely. However, doing so relies on creating well-functioning strategic and operational partnerships based on mutual trust, will and effective process.

Historically, the strategic relationship between the UK government and the cyber insurance industry is best characterised as 'on/off'. As some interviewees from the insurance industry highlighted, the government has taken periodic interest in creating a more meaningful relationship, but often does not follow through on proposals or initiatives.[245] Efforts to generate deeper collaboration have also been hindered by the lack of a single point of contact within government that takes ownership of the relationship.[246] One example highlighted by an underwriter was a 2015 report produced by the Cabinet Office following a period of sustained consultation with insurers, which proposed several recommendations that ultimately went nowhere.[247] However, this was likely a reflection of the

244. DFIR 7, 9 December 2021; breach counsel 2, 9 December 2021.
245. Cyber insurance executive 1, 11 October 2021; insurance industry association 2, 17 November 2021; cyber insurance underwriter 5, 1 November 2021; cyber insurance underwriter 8, 12 November 2021.
246. Underwriter 5, 1 November 2021.
247. Underwriter 8, 12 November 2021. For the Cabinet Office report, see HM Government, 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk', March 2015.

immaturity of the cyber insurance market at that stage as much as of the limitations of the UK government's follow-up work on the report.

At present, the relationship with the UK government is more 'on' than 'off'.[248] The NCSC, for instance, recently developed an Insurance Trust Group with members from the insurance industry and government departments to discuss potential interventions and facilitate data sharing.[249] The impact of this group and other initiatives aimed at developing policy in consultation with the industry remains to be seen.

What has proved even more challenging in both the UK and the US is the development of operational partnerships between law enforcement and cyber security agencies and the insurance industry. Although some interviewees in the UK and the US highlighted that there are meetings between insurers, law enforcement and cyber security agencies to share information, these remained informal at the time of the interviews.[250]

In summary, while it is necessary to be realistic about the effect the cyber insurance market can have on broader efforts to disrupt ransomware, it is also clear that public–private partnerships between the cyber insurance industry and the UK government on ransomware are nascent at best. There is no clear evidence that the cyber insurance industry is having an impact on ransomware reporting, or that the UK government has been able to effectively utilise insurers to support its own efforts. This is partly a problem of incentives – the government has not made a compelling case to the industry on why it should encourage insureds to report, or why insurers should share data. However, it also reflects the lack of well-developed strategic and operational partnerships between the cyber insurance industry and the UK government. The limited size and relative immaturity of the cyber insurance market in the UK also likely contributes to this underdeveloped relationship.

248. Government 1, 29 November 2021; government 2, 1 December 2021; government 4, 10 January 2022.
249. Joint Select Committee on National Security Strategy, 'Written Evidence Submitted by His Majesty's Government'.
250. Underwriter 5, 1 November 2021; cyber insurance claims 1, 28 September 2021; DFIR 6, 23 November 2021.

V. Improving the Role of Cyber Insurance as a Lever to Disrupt the Ransomware Criminal Enterprise

> The answer has to be making it less profitable and more difficult to execute.[251]

This chapter outlines a series of principles and recommendations to help the insurance industry and the UK government and international partners disrupt the ransomware criminal enterprise. These recommendations are not intended to solve all the challenges of the cyber insurance market, nor present wide-ranging solutions to the ransomware challenge. Instead, they focus on where the cyber insurance industry can have the most impact. This reflects the fact that disrupting the ransomware economy involves applying pressure from a variety of different angles in a whole-of-society approach. The recommendations are oriented around the themes identified in Chapters II, III and IV.

Reducing the Profitability of the Ransomware Business Model

Ransom payments sustain the ransomware business model. The high profit margins of ransomware have drawn more cybercriminals into the ecosystem and enabled operators to professionalise and expand their capabilities. Although there is some recent evidence that the number of victims paying and the revenues

251. Underwriter 9, 1 December 2021.

generated may be stabilising or even falling,[252] ransomware remains lucrative for cybercriminals.

One fiercely debated policy option is to legally prohibit ransom payments. There are compelling arguments for and against a ban, but it is not the intention to rehash them here.[253] For now, there is little evidence that the UK government is likely to implement a ban, nor has there been a wide-ranging and formalised policy review with public consultation with the private sector and civil society on the issue.[254]

As an alternative to a blanket criminalisation of ransom payments, some researchers have also advocated for banning insurers from covering ransom payments.[255] However, the research conducted for this paper has highlighted that there is no strong evidence that victims with insurance are much more likely to pay ransoms than those without. Moreover, given that most organisations do not have cyber insurance coverage, such a ban would have little impact on the decision-making of most victims.[256]

A more realistic approach that does not punish victims or limit their ability to recover is to identify interventions that reduce the incentives towards payment and ensure that, when victims do decide to pay, they are able to limit cybercriminals' profits by negotiating more effectively. As highlighted in Chapter II, the insurance industry could play a more active role in reducing the profitability of the business model by instilling ransom discipline in insureds, but this has not yet fully materialised across the market. Several opportunities are yet to be fully exploited by the insurance industry or government to change this dynamic.

252. Chainalysis, 'Ransomware Revenue Down as More Victims Refuse to Pay', 19 January 2023, <https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/>, accessed 8 March 2023.
253. Ransomware Task Force, 'Combating Ransomware', p. 49; Wheeler and Martin, 'Should Ransomware Payments Be Banned?'.
254. Alexander Martin, 'Ransomware Incidents Now Make Up the Majority of British Government's Crisis Management "Cobra" Meetings', *The Record*, 18 November 2022, <https://therecord.media/ransomware-incidents-now-make-up-majority-of-british-governments-crisis-management-cobra-meetings/>, accessed 17 January 2023; Ciaran Martin, 'Lessons from Down Under's Data Disasters Pt. 3', Ciaran's Crispy Cogitations, 17 January 2023, <https://ciaranmartin.substack.com/p/lessons-from-down-unders-data-disasters-78c>, accessed 17 January 2023.
255. Logue and Shniderman, 'The Case for Banning (and Mandating) Ransomware Insurance'; Jan Martin Lemnitzer, 'Why Cybersecurity Insurance Should be Regulated and Compulsory', *Journal of Cyber Policy* (Vol. 6, No. 2, 2021), pp. 118–36.
256. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 52.

Govern the Ransomware Response Ecosystem More Effectively

First, insurers' ability to convene ransomware response services gives them considerable market power. One potential effect of this is that they can reward ransomware response firms that focus on ransom discipline and punish those that do not. However, this task is made more difficult by:

- The lack of clarity over what constitutes best practices in ransomware response and negotiations.
- Insufficient oversight of the incident response and decision-making process.
- Different incentives among different stakeholders involved in ransomware response.
- The absence of assurance and limited regulation around specialist ransomware recovery, negotiation and payment firms.

A starting point is for industry and government to create a better collective understanding of ransomware response best practices, particularly around negotiation protocols and payments. Insurers could contribute to this by using policy language to ensure that insureds and ransomware response firms must provide written documentation of negotiation strategies and outcomes before a claim is paid. The UK government could also contribute to this by commissioning a review of the ransomware response ecosystem that aims to identify key actors in the market and convene them to generate shared knowledge about negotiation protocols. Given that this information may prove valuable for ransomware operators, it should not be distributed beyond trusted industry partners.

Beyond that, the insurance industry, law enforcement and governments should adopt a carrot-and-stick-based approach to firms involved in ransomware response. For instance, insurers should prioritise ransomware recovery firms for their panels that have a proven track record of both achieving outcomes that regularly do not result in ransom payments and working with law enforcement and cyber security agencies. Insurers should also ensure that firms that facilitate ransom payments on behalf of victims meet the highest possible standard in terms of existing regulatory, anti-money laundering and sanctions due diligence and reporting requirements. If making a payment on behalf of a UK victim, these firms should also ideally be registered with relevant financial authorities in the UK.

The UK government should also explore ways to provide more oversight and assurance of firms that provide specialist ransomware response services. The NCSC's existing assurance scheme for incident response providers includes no assessment of their ability to provide specialist ransomware services such as

decryption or negotiations. While this is perhaps unsurprising given the UK government's desire to discourage firms from negotiating or paying, the result is that insurers and ransomware victims are less able to verify the capabilities of specialist ransomware response firms. As such, the NCSC, the NCA and international partners could investigate the feasibility and potential implications of creating a dedicated assurance scheme for specialist ransomware recovery and negotiation firms.

Finally, the UK government and international partners should aim to create a dedicated licensing regime for firms that facilitate ransom payments on behalf of victims. This would not only ensure that payment firms comply with due diligence and reporting requirements, but also ensure that government and law enforcement agencies can collect intelligence on cryptocurrency payments in a much more systematic way. At a minimum, the UK government should seek to follow the example of the US government and ensure that any ransomware response firm or cryptocurrency provider facilitating ransom payments is registered as a money service business in the UK and therefore subject to anti-money laundering reporting requirements.[257]

Recommendation 1: To increase oversight of ransomware response, insurers should use policy language to require that insureds and incident response firms provide written evidence of negotiation strategies and outcomes.

Recommendation 2: To develop and drive ransomware response best practices across the market, insurers should select specialist ransomware response firms for panels that meet a set of predefined minimum requirements. These should include:

- A proven track record of both achieving regular outcomes that do not result in ransom payments, and of operational relationships with law enforcement and cyber security agencies.
- Conducting sanctions risk assessments.
- Compliance with anti-money-laundering laws and FATF standards.
- Ensuring payment firms that make payments on behalf of UK victims are registered with relevant financial authorities in the UK.

Recommendation 3: The UK government should commission a study to improve its understanding of specialist ransomware response firms. This should aim to identify common best practices and key market players, and create a framework for benchmarking the quality of their services and products. These findings can be distributed to trusted partners in the insurance industry. To drive best practices in ransomware response and create more oversight of the incident

257. FATF, 'Countering Ransomware Financing', March 2023, p. 24.

response ecosystem, the NCSC, NCA and international partners should also explore the feasibility and potential implications of creating a dedicated assurance scheme for firms that provide specialist ransomware services such as decryption, recovery, negotiations and payments.

Recommendation 4: To increase reporting of ransom payments, the UK government and international partners should explore creating a dedicated licensing regime for firms that facilitate cryptocurrency payments on behalf of ransomware victims. In the short-term, the UK government should follow the example set by the US government and also ensure that ransomware response firms that facilitate payments are registered as money service businesses in the UK and therefore subject to national financial crime reporting requirements.

Move Towards Payment as a More Clearly Defined 'Last Resort'

Second, there are several interventions that both the insurance industry and government should pursue to ensure victims only pay ransoms as a genuine last resort. Although some interviewees from both the insurance industry and ransomware response firms argued that this is already happening, there are few contractual levers or market-wide best practices to ensure this happens in all cases. This is compounded by the absence of targeted government advice or well-resourced support from law enforcement and government.

As highlighted in Chapter II, increasing the time and options available to victims can encourage them to pursue alternatives to payment. One solution proposed by the Ransomware Task Force is to create a legal requirement for victims to conduct a due diligence review of other options before making a payment.[258] Although governments should explore this recommendation, the insurance industry should also pursue alternative mechanisms. As a starting point, all ransomware coverage should include a set of more rigorous, standardised conditions around crisis management and due diligence that must be met before a ransom payment can be authorised. At minimum, these should include the steps outlined in guidance provided to claims managers by the Lloyd's Market Association in December 2021.[259] Additional conditions could include consulting initiatives such as NoMoreRansom to ensure that decryption keys are not available.[260]

258. Ransomware Task Force, 'Combating Ransomware', pp. 47–48.
259. Lloyd's Market Association, 'Guidance for Handling a Ransomware Incident'.
260. Europol, 'About the Project', <https://www.nomoreransom.org/en/about-the-project.html>, accessed 17 January 2023.

Victims should also be obliged to report to law enforcement before a payment is authorised to access law enforcement support (such as decryption keys which may not be publicly available) and increase intelligence around ransom payments. Although there are good arguments in favour of a mandatory legal reporting requirement for ransom payments in the UK,[261] the interviews conducted for this paper with UK government officials and law enforcement suggested that one is unlikely to materialise any time soon.[262] Given this, insurers should be encouraged to ensure that ransomware coverage includes a law enforcement reporting requirement. However, this should not be treated as a substitute for a robust, evidence-led debate around mandatory reporting of ransomware attacks and payments. One recent precedent UK policymakers could draw on is French legislation that requires victims of cyber attacks to report them to relevant authorities within 72 hours in order to claim on cyber insurance policies.[263]

At the same time, the government must ensure there are more regular positive outcomes for organisations that report. Interventions by the insurance industry and other stakeholders in the private sector must also be backed up by an increase in financial resources for law enforcement and the NCSC to support victims and pursue cybercriminals. This will require resourcing incident management capabilities within the NCSC and law enforcement at greater levels, as well as ensuring ransomware is a higher priority for law enforcement investigations, the criminal justice system and intelligence agencies.[264] At a bare minimum, law enforcement and the NCSC should follow up with all organisations that submit reports and also report back if information provided by victims is used in successful operations against the ransomware ecosystem.

Finally, the government should provide more clarity on what constitutes a legitimate last resort payment. The longstanding line from the UK government and law enforcement is that it 'does not encourage, endorse nor condone the payment of ransom demands'.[265] However, promoting responsible victim behaviour may ultimately rest on acknowledging that there are sometimes legitimate reasons to pay.

Recommendation 5: To reach a market-wide consensus on what constitutes a reasonable last resort before a ransom payment is made, insurers should agree on a set of minimum conditions and obligations in ransomware coverage to

261. Ransomware Task Force, 'Combating Ransomware', pp. 46–47.
262. Government 2; government 3; government 4; law enforcement 1.
263. Orrick, 'France Cybersecurity Update: Cyber-Attacks Must be Reported to Authorities Within 72 Hours to Benefit from Insurance Coverage', 3 February 2023, <https://www.orrick.com/en/Insights/2023/02/France-Cybersecurity-Update-Cyber-Attacks-Must-Be-Reported-to-Authorities-Within-72-Hours>, accessed 8 March 2023.
264. Ransomware Task Force, 'Combating Ransomware', p. 25.
265. NCSC, 'A Guide to Ransomware'.

ensure alternatives are explored first. These should include sanctions due diligence, a requirement to notify law enforcement and written evidence that all options have been exhausted.

Recommendation 6: To increase ransomware reporting and ensure victims are able to access any relevant law enforcement and NCSC support, insurers should specify that any ransomware coverage must contain a requirement for policyholders to notify Action Fraud and the NCSC before a ransom is paid. If there is no progress on this recommendation without intervention, then regulators should intervene to compel insurers to include this obligation in coverage. However, this recommendation also depends on the implementation of long-promised but delayed reforms to Action Fraud. These should include creating a dedicated category for reporting ransomware. Law enforcement and the NCSC must also provide assurances to insurers that they have the capabilities to support victims during incidents and that reporting leads to actual outcomes against ransomware actors, such as cryptocurrency seizures, arrests or offensive cyber operations.

Shift the Narrative on Data Extortion Payments

Third, the rise of data-exfiltration-based extortion has presented a challenge to disincentivising victims from paying ransoms. Although insurers, governments and ransomware response firms have made in-roads in improving victims' ability to recover from back-ups, concerns around litigation, fines and personal and corporate shame resulting from data leaks continue to drive payments.[266]

Confronting this requires sustained messaging and guidance from insurers, government and ransomware response providers that there are considerable risks to paying extortion demands for data protection. At the heart of this should be clear, evidence-based messages about the risks of re-extortion and the fact that victims still need to notify regulators, affected customers and individuals regardless of whether they pay a ransom. Although the NCSC and the ICO have written a joint letter on this subject,[267] government and law enforcement should seek to disseminate this message more widely through public engagement by senior officials and ministers, regional Cyber Resilience Centres and Regional Cybercrime Units, and business associations such as the CBI and the Federation for Small Businesses.

266. RUSI, 'Ransomware Harms and the Victim Experience', <https://rusi.org/explore-our-research/projects/ransomware-harms-and-victim-experience>, accessed 2 July 2023.
267. ICO and NCSC, 'The Legal Profession and its Role in Supporting a Safer UK Online', joint letter, 7 July 2022, <https://ico.org.uk/media/about-the-ico/documents/4020874/ico-ncsc-joint-letter-ransomware-202207.pdf>, accessed 31 December 2022.

Examine the Role of Data Privacy Regulation in the Ransomware Challenge

Finally, the government and the ICO should consider the ongoing unintended effects of privacy regulation on ransom payments. In practice, cybercriminals wield the threat of data privacy fines from regulators to increase pressure on victims to pay. Concerns around the consequences of privacy regulation also give lawyers and some legal considerations an outsized role in ransomware response.

As one recent academic article suggested, the current situation 'requires deep reflection on the objectives of the data privacy regime'.[268] Although proposals around data privacy regulation reforms are outside of the scope of this paper, the government should carefully examine the impact of existing data privacy regulation on ransom payments and even explore options for limiting liability if victims refuse to pay ransomware operators who threaten to leak confidential data. The latter will require careful consideration, as it may conflict with the need to penalise companies that do not take sufficient steps to secure systems and protect personal data.

Raising Costs for Ransomware Operators by Incentivising Cyber Security and Resilience

The insurance industry has played a much more active role in nudging organisations towards better cyber security practices over the past two years. Yet the potential of cyber insurance for reducing the frequency and severity of ransomware attacks is limited by challenges around collecting and assessing reliable cyber risk and forensic claims data. This has proven to be a perennial problem for the industry. In addition, although some insurers are developing increasingly capable threat intelligence and scanning tools that can identify ongoing ransomware campaigns or vulnerabilities, uptake by insureds remains limited due to the lack of contractual obligations and informational barriers. Beyond these insurance-specific challenges, the reluctance of governments and regulators to intervene on compulsory minimum cyber security standards and best practices means that the baseline of cyber security and resilience in the UK and other countries remains low.

268. Baker and Shortland, 'The Government Behind Insurance Governance', pp. 16–17.

One solution mooted by Baker and Shortland involved using technical solutions to collect more 'inside-out' data, such as anomalous network activity or cloud service configurations, through relationships with cyber security firms and cloud providers.[269] There are positive signs that the industry is looking to adopt telemetry-based approaches to underwrite on a more continuous basis,[270] and at least one EDR provider has developed a tool to allow organisations to share internal risk signals with underwriters and brokers.[271] The widespread adoption of this nascent enhanced risk visibility, while it has long been aspirational and technically feasible, depends on improved trust and incentives dynamics between policyholders and insurers/brokers.[272]

Expanding Claims Data Collection

More realistic solutions may, as one analyst recently put it, be 'hiding in plain sight'.[273] As emphasised in Chapter III, the insurance industry has struggled to extract meaningful insights on loss prevention measures from claims data and create a more continuous feedback loop between underwriting and claims. With perhaps the exception of specialist cyber insurers with dedicated incident management capabilities,[274] many insurers are not collecting and optimising digital forensics and incident response data in a systematic way.

Although the insurance industry and the government should explore collective approaches to standardising digital forensics and incident response data across the market, individual insurers should also pursue their own solutions in the short term. The apparent reluctance to share forensic reports with insurers could be partially overcome with tougher policy language that requires policyholders to provide all reports produced by incident response and ransomware recovery vendors. If coupled with investment in more technical expertise in underwriting and claims positions, this should provide a more productive relationship between ransomware incidents and identifying the most relevant

269. *Ibid.*, pp. 44–45; Erin Kenneally, 'Cyber Insurance Sustainability: Learning From the Guy Under the Light Post', Convention Unbound, 17 November 2022, <https://erinkenneally.substack.com/p/d8702373-9c56-4076-9fc8-0740c0f27479>, accessed 20 June 2023.
270. For example, see *Business Wire*, 'Safe Security Launches First Cybersecurity MGA to Underwrite Cyber Insurance Based on Continuous "Inside-Out" Cyber Risk Telemetry', 15 December 2022, <https://www.businesswire.com/news/home/20221215005150/en/Safe-Security-Launches-First-Cybersecurity-MGA-to-Underwrite-Cyber-Insurance-Based-on-Continuous-%E2%80%9CInside-Out%E2%80%9D-Cyber-Risk-Telemetry>, accessed 29 December 2022.
271. SentinelOne, 'SentinelOne Launches WatchTower Vital Signs Report for Cyber Insurers' Risk Management', 25 October 2022, <https://www.sentinelone.com/press/sentinelone-launches-watchtower-vital-signs-report-for-cyber-insurers-risk-management/>, accessed 20 June 2023.
272. Kenneally, 'Cyber Insurance Sustainability'.
273. Kenneally, 'Hiding in Plain Sight'.
274. Underwriter 2, 15 October 2021; cyber insurance claims 2, 11 October 2021; cyber insurance underwriter 8, 12 November 2021.

cyber security controls for underwriting. Defining what this recommendation looks like in practice in the UK context requires more development.

Distribute Government Threat Intelligence and Services via Insurers

The government should seek to exploit the growing scale and reach of specialist cyber insurers in the SME and mid-market by distributing threat intelligence and NCSC services to policyholders. This may also increase the incentive for policyholders to take advantage of services provided by insurers because of the authority associated with the NCSC and the intelligence community more widely.

A starting point could involve integrating some 'active cyber defence' tools into insurers' pre-breach services and intelligence-gathering efforts.[275] Insurers could collect information feeds from the NCSC's Early Warning service on policyholders' IP ranges and then distribute notifications back to policyholders.[276] This would also help develop operational relationships between insurers and the NCSC. However, this may also require improving Early Warning to ensure it can scale to support the large client base that many insurers have.[277]

Recommendation 7: The NCSC and a UK insurer should trial integrating the NCSC's Early Warning service into their ongoing assessments of policyholders. This would enable the insurer to distribute intelligence from Early Warning at scale and notify policyholders of potential ransomware attacks. The NCSC should also explore whether Early Warning will need to be expanded and adapted to meet the requirements of insurers and policyholders.

Supporting Government and Law Enforcement Interventions

Although efforts to increase collaboration between the cyber insurance industry and government and law enforcement have intensified over the last 24 months, there is still considerable scope to create more meaningful operational partnerships and increase ransomware reporting.

275. NCSC, 'Active Cyber Defence: Introduction', <https://www.ncsc.gov.uk/section/active-cyber-defence/introduction>, accessed 17 January 2023.
276. NCSC, 'Early Warning', 11 May 2021, <https://www.ncsc.gov.uk/information/early-warning-service>, accessed 17 January 2023.
277. Claims 2, 11 October 2021.

Create Meaningful Operational Relationships

As a starting point, efforts to create deeper working relationships between cyber insurers and UK agencies could use existing initiatives to further public–private collaboration on cyber security. One example of this is the NCSC's i100 scheme, which brings together public and private sector talent to collaborate on nascent challenges.[278] The NCSC should encourage both underwriters and claims managers to second into the scheme to identify potential areas of operational collaboration and to develop a more open and communicative relationship between the insurance industry and UK government agencies.

Recommendation 8: To deepen operational collaboration with the insurance industry, the NCSC should seek to recruit secondees from the cyber insurance industry into the Industry 100 cyber security secondment scheme.[279] This should include identifying specific tasks and roles for underwriters, claims managers and incident response professionals working for UK insurers.

Increase Reporting of Ransom Payments via Insurers

Limited reporting continues to hamper the development of policy towards ransomware, resource allocation and law enforcement operations. Although the cyber insurance market could encourage policyholders to report incidents through contractual obligations, there are also interventions that could enable insurers themselves play a more prominent role in reporting ransom payments.

At present, the UK does not have a comprehensive framework for reporting and, significantly, tracking ransomware payments. One potential approach is to expand existing financial crime reporting mechanisms to generate insights on ransomware and more actively involve insurers in reporting. Intelligence about ransom payments could be provided through suspicious activity reports (SARs) to the NCA's Financial Intelligence Unit. However, while regulated institutions are required to file a SAR if they detect suspicious behaviour, it is currently not possible to 'code' the SAR as money laundering related to ransomware (although it is possible to code a SAR as relating to virtual assets).[280] Moreover, insurers are not currently covered by existing FATF recommendations and UK money

278. Jamie Collier, 'Optimising Cyber Security Public–Private Partnerships', RUSI Commentary, 28 May 2021.
279. Industry 100 (i100) is a secondment initiative by the UK's NCSC to bring industry and government expertise together. Participating organisations continue to pay staff members' salaries while they are on secondment with the NCSC. See NCSC, 'Industry 100 Inspiring Collaboration', 17 April 2018, <https://www.ncsc.gov.uk/blog-post/industry-100-inspiring-collaboration>, accessed 17 January 2023.
280. National Crime Agency, UK Financial Intelligence Unit, 'Suspicious Activity Report (SAR) Glossary Codes and Reporting Routes', June 2022, <https://nationalcrimeagency.gov.uk/who-we-are/publications/648-glossary-codes-and-reporting-routes-april-2023/file>, accessed 17 January 2023.

laundering regulations, and so may not feel obliged to report. In view of this, the government should explore modifying SARs to incorporate ransomware and find ways to integrate insurers and specialist ransomware response services into financial crime reporting mechanisms.

Recommendation 9: To increase reporting of ransom payments, the Home Office and NCA should ensure that existing financial crime reporting mechanisms – specifically, SARs – are fit for reporting ransom payments or money laundering linked to ransomware. Concurrently, the UK government should also identify ways to encourage cyber insurers to report ransom payments as SARs or through more informal channels.

Conclusions

Ransomware continues to be the most challenging cyber threat that organisations face. At a societal level, it disrupts services that are essential to everyday life. At an individual level, it can ruin lives.[281] This paper has explored cyber insurance's potential contribution to solving the problem.

At present, the evidence is mixed. Cyber insurance is not fuelling the ransomware epidemic by encouraging victims to pay ransoms, but it is also not instilling ransom discipline in insureds across the market. This reflects a lack of collective action on ransomware response and a failure to share best practices more widely.

However, there is growing evidence that insurance is playing a more positive role in raising minimum cyber security standards, particularly among SMEs. This has the potential to make it more difficult and costlier for cybercriminals to compromise organisations. But market penetration for cyber insurance remains low outside the US, which means that cyber insurance is unlikely to improve minimum cyber security and resilience at the scale required to make a significant and lasting impact on the ability of cybercriminals to engage in cyber extortion, at least in the short to medium term. This emphasises that while cyber insurance is currently one of the few market-based levers for incentivising better cyber security practices, it should not be treated as a substitute for minimum cyber security standards, software liability for tech companies, or other potential government interventions in the market.

We should not overemphasise the role of the cyber insurance industry in the fight against ransomware. Just as critics of the industry have overplayed and misunderstood the relationship between insurance and ransom payments, we must not lose sight of the fact that the primary purpose of insurance is to transfer residual risk and cover losses and costs, not to solve cybercrime. Disrupting the ransomware criminal enterprise and changing the risk–reward calculus of Russian cybercriminals in a lasting way will require a mobilisation of government resources, political will and collective action that is yet to materialise.

281. Jamie MacColl, Pia Hüsch and Jason R C Nurse, 'Beyond the Bottom Line: The Societal Impact of Ransomware', RUSI Commentary, 14 November 2022.

Annex 1: Terminology

Cyber insurance: covers the losses relating to damage to, or loss of information from, IT systems and networks.

Cyber threat intelligence: an understanding of cyber threats that can assist the decision-making process.

Double extortion: a form of cyber extortion where threat actors steal sensitive data and threaten to leak it if a ransom is not paid.

Endpoint detection and response (EDR): a cyber security solution that monitors endpoints (for example, computers and other devices) to detect and mitigate cyber threats to them.

Hard market: the upswing in a market cycle, where premiums increase and capacity decreases due to losses or other factors.

Initial access broker: criminal who specialises in obtaining access to organisations' networks.

Insured/policyholder: the buyer and beneficiary of insurance.

Post-breach services: services indemnified or provided by insurers which aim to reduce the impact of cyber security incidents and help insureds recover.

Pre-breach services: cyber security services provided or discounted by insurers which aim to reduce the risk profile of an insured.

Ransomware: activity where threat actors compromise computer systems, demanding a ransom for the restoration or non-exposure of captured, and often encrypted, data and systems.

Ransomware-as-a-service (RaaS): a business model that involves selling or renting ransomware to affiliates, who then share a cut of the profits with the operators that maintain the ransomware and other tools and services linked to it, such as data leak sites and negotiation chat portals.

Ransomware affiliate: criminals who purchase access to RaaS tools and are then responsible for delivering the ransomware payload.

Ransomware operator: criminals who develop and maintain the infrastructure and tools behind ransomware operations.

Soft market: characterised by favourable coverage terms and high availability of coverage.

Threat actors: individuals or groups engaged in malicious cyber activity.

Annex 2: Cyber Insurance and Ransomware Response Services

Cyber insurance policies provide access to and indemnify a range of incident response services relevant to ransomware, including:

- External legal counsel (sometimes referred to as a 'breach coach').
- Digital forensics and incident response (DFIR).
- Crisis management.
- IT recovery.
- Ransomware negotiations.
- Cryptocurrency payment.
- Credit monitoring.
- Public relations.
- Forensic accounting.

Typically, these services are made available through what is routinely described as a panel, which involves specific firms that the insurer has pre-approved.[282] Because these firms gain access to a considerable amount of work through insurance panels, they can be fiercely competitive. The requirements for firms on panels is hard to discern, but typically seem to involve agreeing to specific terms (for example, reduced and/or fixed rates).[283] In some cases, insureds may use firms not on a panel, provided they have prior approval from their insurer, although one cyber insurance broker suggested this was becoming less common due to cost considerations.[284]

In practice, when an insured experiences a ransomware attack, what happens next will depend on how their insurer organises access to its ransomware response services. Through literature and interviews, we identified at least three approaches:

1. **Lawyer-led**. In this model, an insured will call a hotline operated by a third party, typically a law firm or external claims handler. The operator triages the incident

282. Woods and Bohme, 'How Cyber Insurance Shapes Incident Response', p. 5.
283. *Ibid.*
284. Broker 5, 8 December 2021.

and then – at least in an ideal world – recommends specific firms based on the size and severity of the incident. In some cases, the law firms leading this process then subcontract specialist firms (forensics, negotiators, credit monitoring, etc.) on behalf of the insured – what one underwriter described as an 'instant one-stop response' for their clients.[285] This 'lawyer-led' model has become particularly dominant in the US,[286] although interviewees in the UK suggested it is taking hold in Europe due to the impact of privacy regulation and concerns around litigation risk.[287]

2. **Insurer-led**. Much like the above, an insured will call a hotline, but this is operated and triaged by the insurer's claims team rather than a third party.[288] The claims team will recommend suitable firms to respond to the incident, including a third-party law firm or crisis management firm, who will coordinate incident management and other specialist services, even if they are not the first point of contact. This approach is increasingly being adopted by specialist cyber insurers seeking to develop more in-house capabilities to monitor the claims process more closely.
3. **Led by the insurer's incident response firm**. A nascent approach for insurers in the SME market is one where an insurer does not simply act as first point of contact for insureds but may also resolve incidents.[289] This may be either through an in-house incident management function, although this is likely only for very low-impact incidents,[290] or an incident response firm owned by the insurer that is available through their own panel.[291] The extent and impact of this approach on ransomware response remains to be seen, but interviewees and workshop participants suggested more insurers in the SME market will seek to adopt it in order to reduce the costs of incidents.[292]

285. Underwriter 4, 21 October 2021.
286. Woods and Bohme, 'How Cyber Insurance Shapes Incident Response', pp. 10–12.
287. DFIR 4, 27 October 2021; DFIR 3, 21 October 2021; breach counsel 2, 9 December 2021.
288. Claims 1, 24 September 2021; cyber insurance claims 2, 11 October 2021; cyber insurance claims 3, 1 December 2021.
289. Cyber insurance executive 1, 11 October 2021.
290. See CFC, 'Protecting Businesses Against Cyber Attack', <https://www.cfcunderwriting.com/en-gb/cyber/response/>, accessed 26 December 2022.
291. For example, Beazley provides access to Lodestone Security (a security firm it purchased in 2017) through its panel. See Beazley, <https://cyberservices.beazley.com/international/service_providers_international_(en).html>, accessed 27 December 2022. Coalition also provides access to its incident response firm, Coalition Incident Response, through its panel. See Coalition, 'Notice of Available Panel Providers', last updated 28 June 2023, <https://www.coalitioninc.com/panel>, accessed 27 December 2022.
292. Cyber insurance executive 1, 11 October 2021; cyber insurance claims 1, 24 September 2021; cyber insurance claims 3, 1 December 2021.

About the Authors

Jamie MacColl is a Research Fellow in cyber threats and cyber security at RUSI. His research interests include cyber security, the evolution of the cyber threat landscape, the role of emerging technologies in security and defence policy and the uses of history in policymaking. His current research projects focus on ransomware, the concept of cyber statecraft and cyber operations. Prior to joining RUSI, he was a researcher at Orpheus Cyber 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.

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*, BBC and CNN and has provided private briefings on aspects of the cyber threat to high-level forums such as the G7.

Jason R C Nurse is an Associate Professor in Cyber Security in the Institute of Cyber Security for Society (iCSS) & School of Computing at the University of Kent. He also holds the roles of Visiting Fellow in Defence & Security at Cranfield University, UK, and Associate Fellow at RUSI. He received his PhD from the University of Warwick. His research interests include cyber insurance and ransomware, security risk management, corporate communications and cyber security, cyber resilience, and security culture. Jason was selected as a Rising Star for his research into cybersecurity, as a part of the UK's Engineering and Physical Sciences Research Council's Recognising Inspirational Scientists and Engineers (RISE) awards campaign. Dr Nurse has published over 100 peer-reviewed articles in internationally recognised security journals and conferences, and he is a professional member of the British Computing Society.

Gareth Mott is a Lecturer in Security and Intelligence in the School of Politics and International Relations at the University of Kent. Dr Mott's research specialises

in the interchange between technology and software and its socio-political implications. He has conducted research on issues including cyberterrorism, strategies for societal cyber resilience, extremist (mis)use of peer-to-peer technologies, efforts to mitigate ransomware, and the role of 'identity' in the security politics of cyberspace. He convenes a popular research-led module entitled 'Governance and War in Cyberspace' and is an Organisational Lead of the Institute of Cyber Security for Society.

Sarah Turner is a Research Associate and PhD Student in the Institute of Cyber Security for Society (iCSS) and School of Computing at the University of Kent. She is also a Research Fellow at UCL's Knowledge Lab and a Researcher at the 5Rights Foundation, and has been a Research Associate at PETRAS, the National Centre of Excellence for IoT Systems Cybersecurity. Her research looks at how individuals and groups understand and implement aspects of cyber security and data protection practice, both in private, public and corporate settings. She holds an MPA in Digital Technologies and Public Policy from the UCL's department of Science, Technology, Engineering and Public Policy, as well as an MBA, and LLB, and an MA in Literae Humaniores from the University of Oxford. Prior to returning to academia, she spent a decade working in financial services.

Edward Cartwright is a Professor of Economics at De Montfort University and Director of the Institute for Applied Economics and Social Value. His research interests include cyber security, game theory and behavioural economics, with particular interest in the economics of ransomware and the adoption of cyber secure behaviour in micro and small organisations. Recent projects include RAMSES (internet forensic platform for tracking the money flow of financially motivated malware) and EMPHASIS (Economical, Psychological and Societal Impact of Ransomware). He co-developed the Leicester Stories platform and recently supported the East Midlands Chambers of Commerce to establish a Regional Business Intelligence Unit and Collective Intelligence Skills Unit.

Anna Cartwright is a Principal Lecturer in Economics at Oxford Brookes University. She is also a Senior RISCS Fellow on the Theme of Quantification and Cyber Risk. Her research interests include the economics of cyber security, industrial economics and game theory. She led a Home Office-funded project on cyber behaviour in micro organisations that delivered and evaluated cyber security health checks aimed at micro organisations. As a RISCS Fellow, she is leading a research project evaluating the role of local IT companies in disseminating cyber best practice to micro organisations. A particular interest is how to measure and quantify cyber risk in organisations, large and small.