Whitehall Report 2-23

Insurance as Crime Governance: Comparing Kidnap for Ransom and Ransomware

Anja Shortland, Tom Keatinge and and Jamie MacColl

RUSI

Royal United Services Institute
for Defence and Security Studies

Insurance as Crime Governance: Comparing Kidnap for Ransom and Ransomware

Anja Shortland, Tom Keatinge and Jamie MacColl

RUSI Whitehall Report 2-23, March 2023

Royal United Services Institute
for Defence and Security Studies

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 Whitehall Report, March 2023. ISSN 1750-9432.

Cover image: James Thew/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

Executive Summary v

Introduction **1**
Methodology 2

I. Insurance as Governance in Criminal Markets **5**
Making it More Difficult and/or Risky to Commit a Crime 5
Reducing the Cost of a Crime to the Insured/Insurer 6
Reducing the Profitability of a Crime for Criminals 6

II. Practical Application of Loss Management Principles in KfR and Ransomware **7**
Applying Loss Management Principles to KfR 7
Can These Principles be Applied to Cyber Insurance and Ransomware Response? 9

III. Applying Loss Management Principles Online **11**
Making it More Difficult and/or Risky to Commit a Crime 11
Reducing the Cost of Crime to the Insured and Insurer 15
Reducing the Profitability of a Crime for Criminals 16
End Game 20

Conclusion **21**

About the Authors 23

Executive Summary

Ransomware has become a major risk to global business and undermines national economic and societal resilience. Some consider that generous insurance-funded ransom payments are a major contributor to the problem, but many think insurance should be part of the solution. This report therefore examines research activities investigating 'insurance as governance' in the field of extortive crime.

Insurers have a financial interest in limiting the losses they cover. It is commonly known that insurers routinely manage moral hazard and adverse selection among the insured population by incentivising behaviour that limits risk and penalises excessive risk taking. Insurers also create processes that reduce the overall cost of claims by making it more difficult for third parties to benefit from the insurance relationship.

This report applies this approach to insurance as crime governance. The report proposes that insurance measures fall broadly into three categories:

1. Making it more difficult and/or risky to commit a crime.
2. Reducing the cost of a crime to the insured/insurer.
3. Reducing the profitability of a crime for the criminals.

This framework has been tested in a joint workshop organised by RUSI and King's College, London, which was attended by 25 specialists in kidnap-for-ransom (KfR) and ransomware: underwriters, brokers, security advisors, crisis responders and negotiators. KfR insurance is a mature product that has existed since the 1930s. It faced sustainability problems similar to those of the current ransomware epidemic in the past but has since created a sophisticated system to discourage and stabilise kidnapping. By contrast, ransomware coverage, which is generally included in broader cyber insurance packages, is a relatively new product. At the workshop, representatives from both KfR and ransomware response were invited to comment on the extent to which the above governance functions were fulfilled in their sector, where the gaps existed, and what problems needed to be resolved to fill them.

This report finds that the KfR insurance industry has created effective norms and processes to:

- Lower the number of claims by hardening targets.
- Incentivise kidnappers to limit violence against hostages and damage to assets.
- Manage hostage recovery and ensure companies' compliance with duty-of-care standards to prevent costly litigation (thereby reducing the insurance pay out).
- Identify and reward best practice in ransom negotiations and maintain ransom discipline by taking control of negotiations.

- Ensure that participants in the insurance and crisis response market follow established norms and do not compete on terms that could undermine the stability of the overall market.

By contrast, the cyber insurance and ransomware response has:

- Struggled to agree on common minimal cyber hygiene standards, leaving the insured to make their own cyber security decisions. However, the current hard market for cyber insurance is likely to be driving some insureds to become more cautious and resilient. (In a hard market, demand outstrips supply, premiums increase and capacity decreases, due to losses or other factors. In such a market, the insurer has the upper hand when it comes to setting prices or conditions for cover.)
- Not yet arrived at a consensus on what best practice in ransom negotiations is, nor identified tactics to drive down ransoms, especially in the case of data exfiltration.
- In a growing and highly competitive market, failed to create institutions that prioritise the common good over individual self-interest.

Workshop participants agreed that the two crimes and related insurance markets were very different, and that the negotiation protocols developed in KfR could not be used as blueprints for solving the problems of ransomware. However, through taking a broader 'governance system' view, it became clearer which deficits cyber insurance should address as a priority in tackling the ransomware boom. The cyber insurance market must prioritise discovering and disseminating best practice standards for preventing, containing and resolving cybercrime that serve both the market and the public interest, and creating institutions to enforce these broadly (perhaps with the aid of governments).

Introduction

THIS REPORT DETAILS activities that were aimed at comparing and contrasting the response to Kidnap for Ransom (KfR) and ransomware attacks from the point of view of insurers, who have a financial interest in mitigating insured losses. KfR insurance has existed since the 1930s,[1] but the response to KfR, as it is known today, has its roots in the 1970s when kidnap insurers faced the sudden challenge of a kidnap boom in Latin America with exponentially rising ransoms. Since that time, KfR insurance has developed a highly effective private sector-led governance model.[2]

In contrast, the ransomware response industry is much less mature. Although cyber insurance has been in existence since the mid-1990s, this began as an insurance response to cover the costs of liabilities and business interruption incurred by firms expanding into online business.[3] The coverage of ransom response and payments is a much more recent problem.[4] The growth of ransomware has accelerated over the past several years, driven by a permissive environment for Russian cyber criminals, poor cyber-security practices among businesses and public sector organisations, the professionalisation of the ransomware ecosystem, and the development of the cryptocurrency industry.[5] The latter, in particular, has allowed cyber criminals to pair their effective extortion tactics with the opportunity to demand difficult-to-trace ransom payments.

At first sight, there is a significant difference between ransoming people and data. KfR is a very personal and highly emotional crime, preying on human compassion and the natural instinct to protect human life. In contrast, ransomware attacks are conducted remotely and mostly do not threaten lives directly. Yet one should not underestimate the emotional effect on management and staff of seeing businesses disrupted and haemorrhaging money and the impact of this on a business's customers, reputation and brand image. Moreover, physical and cyber attacks can combine social and commercial – whether it is pirates holding ships and crew to ransom or

1. Anja Shortland, *Kidnap: Inside the Ransom Business* (Oxford: Oxford University Press, 2019), pp. 65–67.
2. *Ibid.*
3. Josephine Wolff, *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks* (Cambridge, MA: MIT Press, 2022).
4. Bethan Moorcraft, 'Cyber Insurance Market Reacts to Ransomware Epidemic', *Insurance Business Magazine*, 15 April 2021, <https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-market-reacts-to-ransomware-epidemic-252394.aspx>, accessed 20 March 2023; Tom Baker and Anja Shortland, 'Insurance and Enterprise: Cyber Insurance for Ransomware', *Geneva Papers on Risk and Insurance: Issues and Practice*, 4 December 2022, <https://doi.org/10.1057/s41288-022-00281-7>, accessed 20 March 2022.
5. James Sullivan and James Muir, 'Ransomware: A Perfect Storm', RUSI Emerging Insights, 29 March 2021; Ransomware Task Force, 'Combating Ransomware'.

cyber criminals targeting critical national infrastructure (CNI)[6] or healthcare facilities, putting lives at risk.[7] Both crimes are committed to profit from ransom demands and have spawned an insurance and incident response service aimed at returning people and data to their rightful place. The question, then, is whether the similarities between the two types of ransom demand extend to the tools and methods of those who respond to them.

This report explores potential lessons that the ransomware industry can learn from the more established KfR insurance and response world through research activities, which included a workshop with relevant stakeholders. An online workshop was hosted by RUSI and King's College, London, in June 2022, attended by 25 participants from the KfR and ransomware response industries. Participants identified three key crime control objectives of an insurance-led ransom response:

1. Making it more difficult and/or risky to commit a crime
2. Reducing the cost of a crime to the insured and the insurer.
3. Reducing the profitability of a crime for criminals.

Given that governments and the private sector are still wrestling with ways to mitigate the impact of ransomware on businesses and critical services, exploring lessons learned from KfR in relation to these objectives is both timely and relevant.

This report is divided into three chapters that unpack the topics covered in the workshop, supplemented by prior research. Chapter I looks at how insurance can act as a form of governance in criminal markets in three key ways. Chapter II looks at how this framework has been successfully applied in the KfR insurance industry. Chapter III considers whether this framework can successfully be applied to cyber insurance and ransomware response.

Methodology

This report details the results of a two-hour virtual workshop discussion in June 2022, hosted by RUSI and King's College, London, and attended by 25 participants from the KfR and ransomware response industries representing expertise in physical and cyber security, crisis management ransom negotiations, and insurance. Most participants were based in the UK, with several joining the discussion from the US. However, in both cases, they offered insights beyond these two countries, as the Lloyd's insurance market has global reach, and KfR and ransomware response experts often work on incidents in a wide range of jurisdictions, regardless of where their organisations are based. The authors have also conducted prior research across the KfR and

6. Sergiu Gatlan, 'FBI: Ransomware Hit 649 Critical Infrastructure Orgs in 2021', *Bleeping Computer*, 23 March 2022, <https://www.bleepingcomputer.com/news/security/fbi-ransomware-hit-649-critical-infrastructure-orgs-in-2021/>, accessed 14 September 2022.
7. Kari Paul, '"Lives are at Stake": Hacking of US Hospitals Highlights Deadly Risk of Ransomware', *The Guardian*, 14 July 2022; Kevin Collier, 'Cyberattacks Against US Hospitals Mean Higher Mortality Rates, Study Finds', *NBC News*, 8 September 2022.

ransomware response and insurance fields. The research contributed to several publications, including a 2017 RUSI Occasional Paper examining kidnapping as a source of terrorist finance, a widely acclaimed book, *Kidnap: Inside the Ransom Business*, a study of how insurers at Lloyd's of London have created a well-ordered market that allows the risk to human life from kidnapping to be insured, as well as a 2021 RUSI Occasional Paper considering the increasingly complex and growing challenge posed by cyber risk to governments, businesses and consumers and the potential contribution of cyber insurance to this problem.[8]

It is worth noting that the KfR and ransomware insurance and response industries are replete with acronyms and jargon. This report aims to be accessible to all readers but inevitably some less familiar vocabulary will be used. Unavoidable key terms include: 'insured' – the buyer and beneficiary of insurance provided by an 'insurer'; 'cover' – a frequent term for 'insurance'; and 'hard' – referring to a market in which demand for insurance outstrips supply, giving the insurer the upper hand on setting prices or conditions for cover.

8. Anja Shortland and Tom Keatinge, 'Closing the Gap: Assessing Responses to Terrorist-Related Kidnap-for-Ransom', *RUSI Occasional Papers* (September 2017); Anja Shortland, *Kidnap: Inside the Ransom Business* (Oxford: Oxford University Press, 2019); Jamie MacColl, Jason R C Nurse and James Sullivan, 'Cyber Insurance and the Cyber Security Challenge', *RUSI Occasional Papers* (June 2021).

I. Insurance as Governance in Criminal Markets

WHEN INSURERS CHOOSE to insure clients against a crime, it is often in their financial interest to stabilise or even reduce the frequency and severity of the criminal activity. Scholars in the insurance as governance field observe a wide range of insurance-led developments of norms, processes and institutions to reduce losses.[9] These include efforts to control crime, such as hardening of targets, and increasing the effectiveness of law enforcement.[10] Often, institutions have been created or adapted in response to earlier surges in crime similar to the current ransomware epidemic. Existing literature highlights that insurance-led crime control efforts can be grouped into three broad areas.

Making it More Difficult and/or Risky to Commit a Crime

The aim here is to deter crime and reduce the success rate of criminals. To achieve this, insurers engage with the insured (and the industries on which they rely) to take safety precautions. This may mean encouraging (or mandating) changes in behaviour and investment in security. It can also involve sponsoring or encouraging industries related to the business of the insured to develop and build in technical security solutions, for example, alarms, immobilisers and trackers in the car industry.[11] When insurers are unable to sufficiently influence the behaviour of the insured, they may lobby governments to impose regulation to enforce minimum safety or duty of care standards.

Insurers also engage with governments to provide additional resources for law enforcement to tackle the types of crimes against which they are insuring. In some cases, insurers enter into public–private partnerships with law enforcement, for example, by funding dedicated police units (such as for financial crime and fraud) or creating and maintaining private databases of stolen assets to increase the likelihood of criminals being caught divesting their loot (for example,

9. Richard Ericson, Aaron Doyle and Dean Barry, *Insurance as Governance* (Toronto: University of Toronto Press, 2003); Carol Heimer, *Reactive Risk and Rational Action: Managing Moral Hazard in Insurance Contracts* (Chicago, IL: University of Chicago Press, 1985).
10. Anja Shortland, 'Governing Criminal Markets: The Role of Private Insurers in Kidnap for Ransom Governance', *Governance* (Vol. 31, No. 2, April 2018), pp. 341–58; Kenneth Abraham and Daniel Schwarcz, 'The Limits of Regulation by Insurance', *Indiana Law Review* (Vol. 98, No. 1, 2023); Tom Baker and Anja Shortland, 'The Government Behind Insurance Governance: Lessons for Ransomware', *Regulation and Governance* (2022).
11. Josh Barro, 'Here's Why Stealing Cars Went Out of Fashion', *New York Times*, 11 August 2014.

the National Insurance Crime Bureau car theft database in the US and the international stolen art database maintained by the Art Loss Register[12]).

Reducing the Cost of a Crime to the Insured/Insurer

Insurers can reduce the cost of insured events in three ways. First, they can influence a criminal's incentive to engage in damage limitation, for example, by offering rewards for the return of stolen assets that are in proportion to their value, encouraging criminals (including kidnappers) to minimise violence and harm. Second, insurers may offer services to improve the efficiency of a resolution, for example giving their clients access to professional experts to negotiate settlements with criminals, make payments and recover stolen assets. These experts also ensure that the victims of crime comply with regulatory and duty of care standards to minimise the impact on third parties, and hence liabilities and lawsuits. Third, if insurance covers the cost of business interruption, insurers may offer services to aid the recovery of enterprises after the crime has been resolved.

Reducing the Profitability of a Crime for Criminals

Thefts generally require the sale of the stolen asset for the criminal to make a profit – either on the secondary market or by ransoming them back to the original owner. Insurers have created a multitude of institutions that make the resale of stolen assets riskier for criminals, and stolen objects less attractive to buyers. Examples are markers that make objects unique (such as identification numbers), which can be checked against databases of stolen assets, debit and credit cards, watches and artworks. When these databases are routinely consulted before transactions take place and original owners can demand the return of their assets, the value of stolen assets drops.

Lower prices and riskier 'fencing' (the process of selling stolen goods) may lead criminals to negotiate a direct settlement for the return of the assets to the original owner. Insurers can usefully offer negotiating expertise, help the insured to prepare for such eventualities, and make them more resilient to threats. All these services limit the profit criminals can obtain from negotiated settlements and hence the attractiveness of committing the crime in the first place.

12. Anja Shortland, *Lost Art: The Art Loss Register's Case Book Volume 1* (London: Unicorn, 2021); Tom Baker and Anja Shortland, 'How Insurance Shapes Crime and Crime Shapes Insurance', forthcoming in *Journal of Legal Analysis* (2023), <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4390802>, accessed 30 March 2023.

II. Practical Application of Loss Management Principles in KfR and Ransomware

OVER THE PAST 90 years, KfR insurance and response has formed a sophisticated governance framework of protocols and institutions for loss management. Criminal threats have been countered by institutional innovations designed to stabilise kidnappings and reduce the potential for hostage events to generate extreme losses.[13] This chapter provides an overview of these features.

Applying Loss Management Principles to KfR

When underwriting risks involving complex and hostile territories, KfR insurance is sold through specialist brokers who collect detailed information on the client's risk exposure, such as where, when and how they intend to conduct business in areas with a kidnap risk. This means that insurers select their customers based on their risk/security profile – which is determined by both the innate riskiness of the activity and/or location and the client's risk mitigation measures. Such screening addresses the problem of 'adverse selection', the classic insurance problem that those bearing the highest risks are most keen to obtain insurance. This means that when the price of insurance is raised low-risk customers choose not to be insured, leaving the insurer solely with higher-risk customers and thus a higher likelihood of loss. Where high-risk activities are unavoidable, clients are required to engage the services of security consultancies to mitigate the risks carried by insurers.[14] The result is that many abductions are prevented in the first place, and VIP kidnappings are extremely rare. Kidnappers manage their own risks by focusing on soft targets (such as lower-level local staff, missionaries, sailors, lone reporters, and aid workers), rather than attempting to abduct well-defended foreign key staff, such as technical experts and managers. This approach to risk selection and proactive security reduces both the profit opportunity for criminals and the financial costs for both insureds and insurers. More generally, these measures increase the ongoing resilience of organisations to abductions by building awareness and operational procedures into business practices.

If a kidnap occurs, specialist crisis responders take care of hostage crisis resolutions. Through trial and error, professional negotiators have developed a bargaining protocol designed to protect hostages from torture and death during captivity, encourage fast releases by opportunistic kidnappers (express kidnappings), and minimise ransoms. The first rule of ransom negotiations is to demand proof of life and/or proof of possession from the kidnappers: unless there is a

13. Shortland, *Kidnap*.
14. *Ibid*., *Kidnap*, Chapters 4 and 5.

live hostage and the negotiator is talking to the people who are holding them captive, there is no point in making a payment. Once these basics are established, KfR responders employ a bargaining strategy that emphasises (real or invented) financial and liquidity constraints. They counter outsize ransom demands with much lower offers that rise slowly and in decreasing increments. This encourages kidnappers to release their hostages because eventually the cost of holding them exceeds the expected gain from doing so. During a ransom process there is also a policy of not responding positively to physical threats, which ensures that violence does not pay and hence there is no incentive to escalate it.[15]

While this strategy is heart-rending in the case of the individual hostage, the overall effect is to create order and ransom discipline in the 'market' for hostages. In locations where kidnappings occur regularly, professional negotiators often find stable focal points on which negotiations can converge. Once such expectations are established, holding periods tend to contract – for example, in the Niger Delta the 'going rate' for abducted oil workers was $10,000 for many years, with a holding period of around five days.[16] The bargaining strategy thus makes kidnap resolution relatively predictable, without prioritising speed over safety and cost of settlement. Crisis responders also communicate with each other to ensure that rogue kidnappers are penalised in subsequent attempted transactions. Hostages are used as human shields by their kidnappers. If a gang is known to return live and well hostages, law enforcement generally lets the transaction proceed to preserve lives. However, if the kidnappers routinely kill a high proportion of their hostages during negotiations, the cost–benefit trade-off of an armed rescue may shift towards attempting a liberation.

Once a deal is struck over the ransom amount, further groups of experts manage the payment process and extract hostages alive. Insurance then provides aftercare for hostages and families (such as debriefs, health checks and counselling), minimising the risk of legal repercussions for the actions of the responders.[17]

Thus, KfR insurance works across all three principles of loss management identified above. It makes it more difficult and riskier to abduct hostages and maltreat them. It reduces the overall cost of claims and the profitability of kidnapping. This provides a social benefit in the form of fewer abductions, and those that do occur mostly result in a successful recovery.[18]

KfR insurance also achieves a high level of operational security from those who are covered, as obtaining KfR insurance has become a way for companies to discharge their duty of care towards employees, thus incentivising good compliance with security and crisis response advice, even if the protocol formally leaves the hostage stakeholders (the targeted firm and/or family) in charge of decision-making.[19] Adherence to the bargaining protocol and information sharing within the

15. *Ibid.*, Chapters 6 and 7.
16. *Ibid*., pp. 39, 74.
17. *Ibid*., Chapter 8.
18. *Ibid*., Chapter 11; Shortland and Keatinge, 'Closing the Gap'.
19. Baker and Shortland, 'The Government Behind Insurance Governance'.

industry are enforced and facilitated through an unusual market structure: the overall market is small (with an estimated $400 million per annum in premium income), with the vast majority of kidnap insurance underwritten at Lloyd's of London.

Can These Principles be Applied to Cyber Insurance and Ransomware Response?

In contrast to KfR insurance, which developed with the response to ransom demands at the centre of its design, cyber insurance was developed before ransomware became the significant problem it is today.[20] Ransomware was facilitated by the proliferation of poorly secured or configured IT networks, a lack of commercial incentives for organisations to invest in cyber security, the availability of cryptocurrencies, and geographical safe havens for cyber-criminals.[21]

Cyber insurance was originally mainly required to cover the costs of business interruption, restoring systems and claims for damage arising from privacy breaches and other forms of liability.[22] Even when ransoms were demanded, the amounts were negligible. Thus, as the cyber insurance product was developed, it focused on third-party liabilities, rather than ransom demands.

This approach to loss management was successful in limiting the largest potential source of overall resolution costs. However, it does not address the increasing size and prevalence of ransom demands arising from increasingly sophisticated criminal 'firms' using advanced encryption and data exfiltration capabilities and operating from jurisdictions with weak law enforcement and demanding payment in difficult-to-trace cryptocurrencies.

During the RUSI–King's College workshop, participants considered the extent to which it was appropriate to make the comparisons with the KfR field laid out in the previous section, and whether there were lessons and best practices to share from the KfR response experience.[23]

Contributors from both KfR and ransomware response stressed the differences between resolving hostage crises and ransomware attacks: the emotional responses surrounding threats to life versus commercial interests; the often opportunistic nature of successful ransomware operations versus the deliberate targeting of foreign companies and NGOs for hostages; the greater technical complexity of resolving ransomware incidents and the comparative (un)importance of the ransom in overall resolution costs; the high frequency of ransomware attacks and claims; and the very different market sizes and market structure of KfR versus cyber insurance. It would thus be misleading to overplay either the similarities between these online and offline worlds or the problem-solving potential of applying practices from one area to the other. As one participant

20. Baker and Shortland, 'Insurance and Enterprise'.
21. Sullivan and Muir, 'Ransomware'; Ransomware Task Force, 'Combating Ransomware'.
22. Wolff, *Cyberinsurance Policy*.
23. RUSI–King's College workshop, 13 June 2022.

from KfR response noted, 'this is not about taking the playbook from KfR to cyber and expecting the bad things to go away'.[24]

Yet the large losses on cyber insurance books caused by the recent boom in ransomware has already spawned a range of innovations intended to make cyber insurance more profitable. Several of these are analogous to institutions created in the offline world, although many were developed within the cyber insurance industry and without drawing on the KfR experience. While innovations to stabilise ransomware losses are progressing at a rapid pace, most occur at a company level. Sharing best practice, setting minimum standards and taking collective action has been difficult in this large, highly competitive and fast-growing market.[25]

24. *Ibid*.
25. 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?', *IEEE Security and Privacy* (Vol. 18, No. 1, 2020) pp. 21–27; Erin Kenneally, 'Ransomware: A Darwinian Opportunity for Cyber Insurance', *Connecticut Insurance Law Journal Fall Symposium Edition* (Vol. 28, No. 1, 2021), pp. 165–95.

III. Applying Loss Management Principles Online

THIS CHAPTER CONSIDERS the three loss management principles that emerged from the RUSI–Kings College workshop discussion. It assesses possible and actual insurance approaches to ransomware in more detail, exploring what institutions already exist to make cyber insurance products more resilient, whether further lessons from the offline ransom world could realistically be applied or adapted to combat ransomware attacks, and where completely fresh thinking is needed.

Making it More Difficult and/or Risky to Commit a Crime

Improving Cyber Risk Management Practices

Improving an organisation's cyber security posture can make it more difficult for ransomware operators to gain access to victims and deploy ransomware or exfiltrate data. Good cyber risk-management practice closes off easy entry points, limits the lateral movement of hackers inside a company's systems, keeps the most sensitive data confidential, and creates timely and accessible backup solutions. Just as KfR insurers require clients to undergo security assessments, hostile environment training and other forms of awareness raising, so too might cyber insurers require clients to undergo comparable training to reduce the risk of a ransomware attack gaining access to a company in the first place.

Security Requirements

Despite the rapid expansion in security advisories on best practice in response to ransomware attacks, the cyber insurance industry has in the past come under criticism for lax underwriting standards around security.[26] In what has historically been a competitive market, insurers have been reluctant to impose strict security standards, although in the current hard market minimum security requirements – notably multi-factor authentication, endpoint detection and response, and strong backup processes – have emerged.[27] This is a step in the right direction, although there

26. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'; Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?'.
27. RUSI–King's College workshop; for specific examples, see Howden, 'Cyber Insurance: A Hard Reset 2.0', 2022, <https://www.howdengroupholdings.com/assets/documents/howden-cyber-insurance-a-hard-reset-2.pdf>, accessed 14 September 2022; Phil Muncaster, 'Number of Firms Unable to Access Cyber-Insurance Set to Double', *Infosecurity Magazine,* 9 August 2022, <https://www.infosecurity-magazine.com/news/firms-unable-access-cyberinsurance/>, accessed 14 September 2022; Jenni Bergal, 'Cyber Insurance Price Hike Hits Local Governments Hard',

are still unanswered questions about the robustness of the evidence base that underwriters are using to set security requirements.[28] This connects to a more fundamental problem that limits the industry's collective ability to mitigate the threat from ransomware – namely, the lack of consensus and reliable data about what measures actually improve cyber security.

During the workshop discussion, it was also clear that there is no standardised approach to underwriting cyber risk – indeed, fundamentally different approaches exist.[29] The nascent nature of the market and the dynamic nature of cyber risk means that providers will likely continue to experiment with different underwriting approaches around security controls.

Pre-Breach Training

The online world is also developing crisis management and incident response training – a staple of hostage crisis resolution. Workshop participants involved in ransomware response stressed the complexity of resolving and recovering from cyber attacks, which require a wide range of expertise from within and outside organisations.[30] Training makes organisations more resilient to cyber attacks. Identifying the incident response team and working through various scenarios beforehand facilitates damage limitation, ensures that the business has a clear negotiation strategy, and streamlines the recovery process.

Although crisis management training and other types of pre-breach security services are often available from insurers, cyber insurance underwriters in the workshop highlighted that many insureds choose not to take up these services.[31] As a general rule, most victims still only contact their insurer post-breach.

Proactive Threat Intelligence

Another area where the cyber insurance industry has developed similar capabilities to the offline world is in the proactive development and dissemination of threat intelligence.[32] Some insurers are collecting and sharing knowledge about initial access vectors currently being used by threat actors. This has been enhanced by the uptake of attack surface monitoring within the cyber insurance industry, which allows insurers to scan for and identify some vulnerabilities and cyber hygiene practices in insureds' internet-facing infrastructure. For example, in 2021–22,

---

The Pew Charitable Trusts, 27 July 2022, <https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2022/07/27/cyber-insurance-price-hike-hits-local-governments-hard>, accessed 14 September 2022.

28. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge'; Daniel Schwarcz, Josephine Wolff and Daniel Woods, 'How Privilege Undermines Cyber Security', *Harvard Journal of Law and Technology* (Vol. 36, No. 2, 2023).
29. RUSI–King's College workshop.
30. *Ibid*.
31. *Ibid*.
32. MacColl, Nurse and Sullivan, 'Cyber Insurance and the Cyber Security Challenge', p. 22.

many cyber insurers recognised their exposure to the Log4J vulnerability. They quickly moved to advise their clients to assess their risk and remediate the vulnerability.[33]

The broad adoption of this approach would help raise awareness of current weaknesses, particularly for small and medium-sized enterprises (SMEs). As with other elements of the cyber insurance market, however, varying levels of maturity and technical expertise mean that there is no standardisation in the provision of threat intelligence, and the quality of services varies significantly from carrier to carrier. As with other types of pre-breach services, workshop participants from the cyber insurance industry also highlighted that it is difficult to incentivise insureds to act upon threat intelligence.[34] The fact that most SMEs outsource their IT management to managed service providers or other third parties also likely contributes to this problem as it increases the disconnect between insurers and those managing IT and cyber security.

Whereas the three points above focus on making it more difficult for cyber criminals to launch their attacks successfully, making it riskier to commit the crime in the first place should also be considered in order to deter would-be ransomware operators.

The Role of Law Enforcement

The KfR response industry has, by necessity, developed close relationships with law enforcement. While law enforcement is critical in the prevention of kidnaps, rescue attempts can be a much riskier option than a well-managed professional ransom negotiation. Crisis responders thus prefer police or military forces to delay intervention activities until after the hostage has been released, but will collect and provide information to help catch the criminals and reduce the likelihood of further abductions.[35]

For the cyber insurance community, it is likewise the case that incident response experts trying to get a client back online as fast as possible have different priorities when dealing with ransomware cases from the police, who may slow down the resolution of a ransomware attack and impede recovery as they prioritise gathering evidence as part of broader investigations into ransomware groups.[36] This misalignment of incentives conflicts with the interests of the insureds and insurance companies. Developing a more effective modus operandi with law

33. Ayelet Kutner, 'Security Alert: Log4j', At-Bay, 14 December 2021, <https://www.at-bay.com/articles/security-alert-log4j/>, accessed 13 March 2023; CFC Underwriting, 'Client Advisory: Log4Shell Vulnerability', 13 December 2021, <https://www.cfcunderwriting.com/en-gb/resources/advisories/2021/12/log4shell/>, accessed 13 March 2023.
34. RUSI–King's College workshop.
35. In cases where hostages are taken by terrorist groups, legislation prohibiting the payment of ransoms, in line with terrorist-financing prohibitions, means that the capacity for KfR responders to negotiate is extremely limited. In these cases, military action is likely to be one of a few limited options open to the governments of those citizens who have been kidnapped. For an extensive discussion of this issue, see Shortland and Keatinge, 'Closing the Gap'.
36. RUSI–King's College workshop.

enforcement is one area where the cyber insurance industry is still working out how to develop strategic relationships with law enforcement.[37]

The Role of Governments

In recent years, government focus on ransomware has grown. The US has led the way, with initiatives such as the Ransomware Taskforce and the publication of advisories from financial crime[38] and cyber security government agencies,[39] in partnership with allies.[40] However, governments have shied away from regulating or mandating minimum cyber hygiene standards. There is no equivalent of the duty of care standards to which businesses are held to protect their employees from physical harm, which can be leveraged by insurers to secure better engagement and compliance on security.

As in the KfR field, governments' sanctions regimes have complicated matters for ransomware response. Sanctions cause significant uncertainty over the reimbursement of ransom payments, as it is difficult to positively identify online perpetrators. State-directed (condoned or deniable) cyber operations are also beginning to affect the cyber insurance realm and by necessity attract greater attention from governments. Insurers already exclude tail risks, such as 'war', from their policies and hand these risks back to insureds and, ultimately, governments.[41] It seems probable that the proportion of these types of attack will rise in the future.

The Role of Intelligence and Security Agencies

In view of the centrality of technology and cyber security to national security, intelligence and security agencies apply increasing focus to the field of cybercrime, and may deploy their capabilities against cyber criminals, particularly in response to the disruption of CNI and as

37. Jeff Stone, 'FBI Turns to Insurers to Grasp the Full Reach of Ransomware', *Cyber Scoop*, 30 March 2020, <https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/>, accessed 13 March 2023.
38. See FinCEN, 'Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments', FIN-2021-A0048 November 2021, <https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf>, accessed 23 August 2022.
39. See CISA, 'CISA, FBI, NSA and International Partners Issue Advisory on Ransomware Trends from 2021', 9 February 2022, <https://www.cisa.gov/news/2022/02/09/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021>, accessed 11 October 2022.
40. FBI, CISA, ACSC, NCSC-UK, '2021 Trends Show Increased Globalized Threat of Ransomware', Joint Cybersecurity Advisory, 9 February 2022, <https://www.ncsc.gov.uk/files/2021%20Trends%20show%20increased%20globalised%20threat%20of%20ransomware.pdf>, accessed 23 August 2022.
41. Lloyd's Market Association, 'Cyber War and Cyber Operation Exclusion Clauses', 25 November 2021, <https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx>, accessed 20 March 2023.

the state-criminal nexus aspect of ransomware grows.[42] In response, ransomware groups have themselves developed their own resilience capabilities, as although in certain countries the threat of arrest is low, the threat of infrastructure disruption through offensive cyber operations is credible.[43] As some insurers aggregate data on ransomware groups (such as cryptocurrency payment wallets), such data could be used by intelligence and security agencies to inform or prioritise operations.

In sum, with the limited exception of being sanctioned or indicted, ransomware operators face a low likelihood of any sort of repercussion for their activities and, where there is law enforcement intervention, this may conflict with the efforts of ransomware response companies and insurers.

Reducing the Cost of Crime to the Insured and Insurer

As noted above, cyber insurance was originally developed with the principle of reducing the cost to both insured and insurer of ransom crime in mind, but focused in particular on containing the costs related to liability claims resulting from cyber attacks. The effectiveness of applying this philosophy to ransomware response remains mixed, and criminals are skilled at adapting their tactics in response. Once a cyber criminal is inside a target's network, the extent to which they can cause damage depends on their ability to move laterally through the target's systems and encrypt and secure sensitive data. Furthermore, a key tenet of a ransomware attack is that the data targeted is unique, and thus the victim has no alternative but to pay if they want to retrieve it. However, workshop participants involved in ransomware response made it clear that in recent years insureds have made huge strides in making easily accessible and useable backups, in part because insurers have required better resilience measures.[44] This has allowed many victims to recover without paying a ransom.[45] As a result, and consistent with the continuous evolution of the cyber threat landscape, ransomware operators have moved to not only deny access to data but also exfiltrate sensitive information and blackmail targets with publication.

The cost of attacks can also be reduced and a business restored online via the rapid containment of an attack and the closure of initial access vectors, along with the swift resolution of the event via negotiations with the criminals, while ensuring compliance with regulatory requirements. Although this is an individually rational approach to limit the cost of each attack, it is not socially

42. Corin Faife, 'Former Conti Ransomware Gang Members Helped Target Ukraine, Google Says', *The Verge*, 7 September 2022, <https://www.theverge.com/2022/9/7/23341045/former-conti-ransomware-gang-target-ukraine-google>, accessed 14 September 2022; Christopher Bing and Andy Sullivan, 'US Charges Three Iranians for Ransomware Attacks on Women's Shelter, Businesses', *Reuters*, 14 September 2022.
43. RUSI–King's College workshop.
44. *Ibid*.
45. Coveware, 'Improved Security and Backups Result in Record Low Number of Ransomware Payments', <https://www.coveware.com/blog/2023/1/19/improved-security-and-backups-result-in-record-low-number-of-ransomware-payments>, accessed 26 March 2023.

optimal: fast and generous ransom payments incentivise further attacks and the growth of ransomware crime.

Reducing the Profitability of a Crime for Criminals

Most cyber insurers offer their clients access to professional incident response services, with a focus on reducing the total cost of each incident. Workshop participants highlighted that for some ransomware negotiators, the KfR industry has provided a helpful framework for shaping their approach to ransom negotiations. Yet it can be difficult to defy the commercial interests of victims, who weigh the relatively minimal cost of ransom payments against the considerable cost of business interruption. As one ransomware negotiator in the workshop noted, 'It is difficult to advise an anxious CEO to slow down ransom response negotiations when their firm is haemorrhaging money'.[46] What is lacking so far, therefore, is a sense of collective responsibility to achieve ransom discipline to reduce the profitability and hence the attractiveness of committing the crime.

To Negotiate … or Not?

As in KfR, the first rule of negotiation is to demand 'proof of life'. Ransomware victims have learned the hard way that not all decryption works once a ransom has been paid.[47] Whereas proof of life in KfR can be achieved via a telephone call with the victim or via obtaining information that only the victim knows, getting genuine proof of life and proof of possession is not as simple in ransomware cases. Criminals may try to pass off uncorrupted exfiltrated files as proof that they can restore encrypted data.[48] Crisis responders have therefore been collecting and sharing information about threat actors' performance and credibility in decryption.[49] Thus, ransomware groups with poor decryption records are likely to be met with more resistance when they make their demands and may not receive payment, on the grounds that they are untrustworthy.

46. *Ibid*.
47. Kaspersky, 'Consumer Appetite Versus Action: The State of Data Privacy Amid Growing Digital Dependency', Kaspersky Consumer IT Security Risks Report 2021, <https://www.kaspersky.com/about/press-releases/2021_over-half-of-ransomware-victims-pay-the-ransom-but-only-a-quarter-see-their-full-data-returned>, accessed 11 October 2022; Coveware, 'Dharma Ransomware Recovery Rates Fall as Ransom Demands Skyrocket', 21 March 2019, <https://www.coveware.com/blog/dharma-ransomware-datarecovery-rates-are-decreasing-as-ransom-demands-increase>, accessed 14 March 2023.
48. RUSI–King's College workshop.
49. See, for example, Coveware, 'Ransomware Victims Hit by Abandoned GlobeImposter TOR Site', 6 December 2018, <https://www.coveware.com/blog/2018/12/6/abandoned-globeimposter-tor-site-leaves-ransomware-victims-without-options>, accessed 11 October 2022.

If there is proof of life, the next question is whether to engage in a ransom negotiation. This can sometimes be avoided by using publicly available decryption and removal tools.[50] However, the constant development and evolution of ransomware strains means these tools are often not relevant for many victims. Having regularly updated offline backups that are readily accessible also gives firms an alternative to paying criminals for decryption keys.

However, the shift to data exfiltration has complicated the decision-making process for firms. As well as investigating or demanding what data has been encrypted, victims in many cases must now also understand how commercially or personally sensitive this data is, given the threat of exposure. Some workshop participants highlighted that victims are much more likely to pay in cases of double extortion (where data is both encrypted and exfiltrated) because of concerns around liability exposure and reputational damage. This risk may be mitigated if a firm is resilient to having stolen data published or if the reputational cost of suffering a ransomware attack is reduced by 'breach fatigue'.[51] As cyber security breaches become the norm rather than the exception, media coverage of attacks and the stigma of having failed to protect data may be lessening.[52] This might in time reduce the amount that firms are willing to pay to avoid exposure and hence the leverage criminals can derive from this tactic.

One suggestion made during the workshop by a participant working in ransomware response was that ransomware victims who refuse to pay a ransom could be further protected by governments by having their exposure to third-party liability and other related claims limited in return – for example, by governments amending legislation to make it more difficult for class actions to be filed or by only reimbursing actual damages, rather than imposing punitive fines on the breached company. Other participants noted that guidance from regulators is mixed, as some regulators have been known to demand that ransom payments are made in order to prevent the leaking of private data.

Negotiation Quality

If a negotiation is indeed the most effective and efficient way of recovering from an attack, the question is how large a ransom should be paid.[53] In the KfR field, there is a general understanding that paying high ransoms drives up resolution costs across the board and can cause a kidnapping

50. See, for example, Coveware, 'Decrypt GandCrab Ransomware: How to Recover GandCrab Encrypted Files', <https://www.coveware.com/blog/gandcrab-diy-guide-to-decryption>, accessed 11 October 2022.
51. Security Intelligence, 'Data Breach Fatigue Makes Every Day Feel Like Groundhog Day', <https://securityintelligence.com/data-breach-fatigue-makes-every-day-feel-like-groundhog-day/>, accessed 26 March 2023.
52. RUSI—King's College workshop.
53. At the same time, there may be value in negotiating even if a victim does not intend to pay a ransom, as it can buy them time to investigate and remediate without further damage being caused by the attacker.

boom. KfR negotiation protocols are well established and mapped out in advance, with a goal of maintaining ransom discipline.

In contrast, ransomware negotiation protocol is still emerging and varies across the industry, with negotiations conducted on a more ad-hoc basis. This is partly a result of a lack of experience. One ransomware negotiator who previously worked at a security consultancy that also offered KfR negotiation services said at the workshop that their early efforts at negotiating with ransomware operators were 'embarrassing' when compared to the firm's detailed and methodical protocol for dealing with kidnappers.[54]

Another challenge is the lack of collaboration across the ransomware response industry (in stark contrast to the KfR response community).[55] The KfR response market is a small and cooperative community that shares information easily. Good negotiators are identified and rewarded by the market; unsuccessful ones are sidelined. Ensuring the quality and consistency of ransomware negotiators is a clear lesson that the ransomware industry can learn from the KfR community. However, the size of the cyber insurance market and the frequency of ransomware attacks means applying this lesson will be difficult.

To do so, the industry will first need to define good practice in ransomware negotiations. For example, does good practice relate to the 'discount' negotiators can obtain from criminals and how the ultimate payment compares to the cost of business interruption? 'Good' for the customer may not be 'good' from the point of view of the overall market, as a negotiator may achieve success – the return of data in a speedy fashion – at the expense of ransom payment market discipline and with subsequently raised future ransomware payment expectations. In KfR, this tension has been overcome by collective action. All market participants occasionally conduct long and stressful negotiations where the cost of running down the clock on the kidnappers is much higher than the 'savings' from slightly reducing the ransom. However, everyone in the market benefits from the ransom discipline and the affordable focal points generated by such tough bargaining.

Creating ransom discipline will also require the ransomware industry to identify and commercially sideline 'bad' ransomware negotiators. Certain examples have highlighted that some negotiators directly benefit financially from relationships with ransomware operators: a ransomware negotiator shared the ransom payment with the criminals behind the Hive ransomware operation,[56] while the Conti leaks[57] refer to 'friendly negotiators' working for

54. RUSI–King's College workshop.
55. *Ibid*.
56. Kendall McKay, 'Conti and Hive Ransomware Operations: Leveraging Victim Chats for Insights', Cisco Talos, 2 May 2022, p. 8, <https://blog.talosintelligence.com/conti-and-hive-ransomware-operations/>, accessed 11 October 2022.
57. The Conti leaks involved either a disgruntled member of the Conti ransomware operation or a security researcher leaking chat logs.

ransomware recovery firms that actively advised the group how to extract higher ransom payments from victims.[58]

Negotiation Strategy

KfR has, from experience, identified time as the pain point for kidnappers (it always is for the victims). Holding hostages is costly, saddling kidnappers with costs (security, food and other forms of support) that they cannot fulfil without a ransom. In extremis, hostages may die, rendering them valueless for negotiations. Time also allows law enforcement and security agencies to collect information and conduct investigations which may lead to a rescue mission, removing the kidnappers' financial opportunity.

Currently, given the mixed record of law enforcement on responding robustly to ransomware attacks, it is unclear whether there is an equivalent pain point for cyber criminals. Data kidnappers have few pressures to conclude a negotiation. Attribution and indictments of specific criminals,[59] sanctions,[60] arrests (outside Russia),[61] and disruption of ransomware operators' infrastructure have all had some impact,[62] but the scale of their operations and the relatively cost-effective nature of cyber attacks mean that criminals can move on to other targets very quickly without needing to resolve an existing case first.

Nonetheless, several workshop participants who work in ransomware response stressed that increasing the length of negotiations generally means they can reduce the ransom demand or even remediate an incident without paying a ransom.[63] Hackers that have exfiltrated terabytes of data have to pay to store this data, and there always is the possibility that their victim is

58. Brian Krebs, 'Conti Ransomware Group Diaries, Part III: Weaponry', Krebs on Security, 4 March 2022, <https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/>, accessed 11 October 2022.
59. US Department of Justice Office of Public Affairs, 'Ukrainian Arrested and Charged with Ransomware Attack on Kaseya', 8 November 2021, <https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya>, accessed 20 March 2023.
60. Danny Palmer, 'Ransomware has Gone Down Because Sanctions Against Russia are Making Life Harder for Attackers', *Zdnet*, 10 May 2022, <https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/>, accessed 11 October 2022.
61. Interpol, 'Joint Global Ransomware Operation Sees Arrests and Criminal Network Dismantled', 8 November 2021, <https://www.interpol.int/en/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled>, accessed 20 March 2023.
62. Julian E Barnes, 'US Military has Acted Against Ransomware Groups, General Acknowledges', *New York Times*, 5 December 2021.
63. This is supported by empirical evidence. See DIFR Research Group and Team Cymru, 'Analysing Ransomware Negotiations with CONTI: An In-Depth Analysis', <https://difr.unipi.gr/docs/conti.pdf>, accessed 11 October 2022; BakerHostetler, 'Baker Hostetler Launches 2022 Data Security Incident Response Report: Resilience and Perseverance', 7 April 2022, <https://www.bakerlaw.

developing a work-around and only negotiating half-heartedly. These vulnerabilities are already being successfully exploited by some leading ransomware negotiation firms.

End Game

A final area of comparison – and material difference – relates to the conclusion of a ransom situation. When a KfR incident is concluded successfully, the hostage is returned alive. In contrast, in a ransomware situation, even if stolen data is returned, the victim can never be sure that their data has not been copied and sold or stored for a future round of extortion.[64] This raises the question of the extent to which 'trust' can be developed between negotiators and criminals in the cyber realm, given the ephemeral nature of ransomware gangs.

In summary, the RUSI/King's College workshop and the authors' research demonstrate that there are already impressive pockets of excellence in cyber insurance across all areas of loss management. Even if cyber response has not learned directly from the KfR field, the market leaders follow similar intuitions and adopt protocols that often look like close cousins of their KfR counterparts. Some (niche) insurers carefully select and price their risks based on a detailed understanding of their clients' security profile, while others work closely with cyber security providers to give proactive advice and pre-incident training to their customers. More and more firms protect sensitive data and have invested in reliable backup solutions, reducing the need to cooperate with criminals. The industry leaders in ransomware resolution only negotiate when the hackers have provided both proof of life and proof that they can reverse the encryption. Good negotiators can significantly reduce ransom demands, although there are areas that still require improvement and ideas on how to change the game. The main difference between the two markets is that KfR has been successful at turning good and best practice into an industry standard, whereas in cyber insurance firms currently make their own choices – often at the expense of future victims.

com/BakerHostetler-Launches-2022-Data-Security-Incident-Response-Report-Resilience-and-Perseverance>, accessed 11 October 2022.

64. RUSI–King's College workshop.

Conclusion

THIS REPORT HAS drawn on a RUSI–Kings College workshop involving industry experts that debated the lessons that could be learned by cyber insurers from the experience of the KfR community in dealing with hostage taking and negotiation. The debates revealed a mixed picture.

The criminal pursuit of financial gain through the collection of a ransom is core to both KfR and ransomware. The pressure on victims of ransomware to pay leverages the desire to protect a valuable commodity. However, in KfR both the value placed on a hostage's life and the emotional strain on kidnappers of keeping a hostage in captivity for another day, week or month are private information that can be hidden from the hostage-takers. And each extra day of captivity comes at a cost to the kidnappers. This creates scope for exerting downward pressure on any ransom. By contrast, the (potentially huge) cost inflicted on firms through data disruption is evident to ransomware attackers and extending negotiations generally harms the victims more than the perpetrators. This creates strong pressures for fast payments that resolve the immediate problem – but also fuel further attacks.

High-quality security comes at a cost in both the ransomware and KfR fields. Firms know how to make things more difficult for would-be attackers in both scenarios, but cyber insurers have so far been reluctant to set or enforce cyber security standards. Partly this is because ransomware attacks are more random than kidnappings. There are countless access vectors across the globe to data, rather than known hotspots and modes of hostage-taking activity. The evolutionary nature of cyber risk and the dynamic threat landscape may limit the ability of the insurance industry to standardise up-to-date best practices. But even basic cyber hygiene has historically been neglected in the desire for cyber insurers to increase market share in this growing and fiercely competitive market, as they fail to impose too many burdens on their clients in terms of taking precautions.

Interrupting the dynamics of ransomware requires collective action among insurers. However, the cyber insurance and response industry is a much larger market than KfR, and the sort of decentralised governance that has served the latter so well is far more difficult to establish here. Nevertheless, insurers, businesses and societies would greatly benefit from improved information sharing and collaborative efforts to improve negotiation protocols and help law enforcement to pursue the criminals. Recognising that the comparison between the two industries should not be overplayed, it is noted that there are many excellent loss prevention and loss mitigation initiatives in the ransomware domain. These are closely related to best practice in the KfR field, although they may have been developed independently and without reference to KfR. There are also ongoing efforts and early successes in improving negotiation tactics to drive down ransoms. The problem is that best practice is not shared or emulated widely. Although cyber insurers know how to improve outcomes, doing so is only commercially

viable when their competitors adopt the same standards. Therefore, the most important lesson from KfR that is yet to be learned is the importance of acting collectively for the greater good of the overall market and society. The current hard market for cyber insurance pricing and the high political salience of ransomware may provide a window of opportunity for this coordination to be further developed.

About the Authors

Anja Shortland is a Reader in Political Economy at King's College London. Her current research projects are in peace science and the economics of crime. Although often based on data analysis, her work usually cuts across disciplinary boundaries, adopting techniques and insights from sociology, engineering, geography, politics, international relations and economics. Anja was an Engineering and Economics undergraduate at Oxford and completed her Master's and PhD in International Relations at the London School of Economics. Before moving to King's, she worked as a lecturer in Economics at Leicester, a reader in Economics at Brunel University and as a consultant to the World Bank.

Tom Keatinge is the Director of the Centre for Financial Crime and Security Studies at RUSI.

Jamie MacColl is a Research Fellow in cyber threats and cyber security in the Centre for Financial Crime and Security Studies at RUSI. His research interests include ransomware, the evolution of the cyber threat landscape, the role of emerging technologies in security and defence policy and the uses of history in policymaking.