RUSI
Royal United Services Institute
for Defence and Security Studies

University of Kent

supported by National Cyber Security Centre

RISCS
Research Institute for Sociotechnical Cyber Security

Occasional Paper

Cyber Insurance and the Cyber Security Challenge

Jamie MacColl, Jason R C Nurse and James Sullivan

Cyber Insurance and the Cyber Security Challenge

Jamie MacColl, Jason R C Nurse and James Sullivan

RUSI Occasional Paper, June 2021

Royal United Services Institute
for Defence and Security Studies

190 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 190 years.

Published in 2021 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, June 2021. ISSN 2397-0286 (Online).

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 RUSI team that helped to guide and shape this paper. Sneha Dawda, Chris Goodenough, Hugh Oberlander, Dina Mansour-Ille, Demi Starks, Zenab Hotelwala, Tom Sayner and Sarah Hudson all provided valuable support and editing. The authors would also like to thank Rebecca Lucas, formerly of RUSI, for her outstanding work on the literature review and other data collection that helped form the basis of much of the paper.

Thanks also go to Josephine Wolff, Graham Walsh and Ioannis Agrafiotis for peer reviewing the paper with such diligence, as well as the various individuals from government, the insurance industry and cyber security providers who provided insightful feedback on 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 when 2020 and 2021 were and continue to be challenging for us all. Every single interview contributed greatly to the authors' thinking and findings.

Executive Summary

GOVERNMENTS AND BUSINESSES are struggling to cope with the scale and complexity of managing cyber risk. Over the last year, remote working, rapid digitalisation and the need for increased connectivity have emphasised the cyber security challenge. As the pursuit of approaches to prevent, mitigate and recover from malicious cyber activity has progressed, one tool that has gained traction is cyber insurance. If it can follow the path of other insurance classes, it could play a significant role in managing digital risk.

This paper explores whether cyber insurance can incentivise better cyber security practices among policyholders. It finds that the shortcomings of cyber insurance mean that its contribution to improving cyber security practices is more limited than policymakers and businesses might hope. Although several means by which cyber insurance can incentivise better cyber security practices are identified, they have significant limitations. Interviewees from across government, industry and business consistently stated that the positive effects of cyber insurance on cyber security have yet to fully materialise. While some mature insurers are moving in the right direction, cyber insurance as a whole is still struggling to move from theory into practice when it comes to incentivising cyber security.

If this is to change, the insurance industry must overcome significant challenges. One is the competitiveness of the nascent cyber insurance market over the last two decades. Most of the market has used neither carrots (financial incentives) nor sticks (security obligations) to improve the cyber security practices of policyholders. The industry is also struggling to collect and share reliable cyber risk data that can inform underwriting and risk modelling. The difficulties inherent in understanding cyber risk, which is anthropogenic and systemic, mean insurers and reinsurers are unable to accurately quantify its causes and effects. This limits insurers' ability to accurately assess an organisation's risk profile or security practices and price policy premiums accordingly. The spectre of systemic incidents such as NotPetya[1] and SolarWinds[2] has also limited the availability of capital for cyber insurance markets.

However, the most pressing challenge currently facing the industry is ransomware. Although it is a societal problem, cyber insurers have received considerable criticism for facilitating ransom payments to cybercriminals. These add fuel to the fire by incentivising cybercriminals' engagement in ransomware operations and enabling existing operators to invest in and expand their capabilities. Growing losses from ransomware attacks have also emphasised that the current reality is not sustainable for insurers either.

---

1. Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.
2. Dina Temple-Raston, 'A "Worst Nightmare" Cyberattack: The Untold Story of the SolarWinds Hack', *NPR*, 16 April 2021.

To overcome these challenges and champion the positive effects of cyber insurance, this paper calls for a series of interventions from government and industry. Some in the industry favour allowing the market to mature on its own, but it will not be possible to rely on changing market forces alone. To date, the UK government has taken a light-touch approach to the cyber insurance industry. With the market undergoing changes amid growing losses, more coordinated action by government and regulators is necessary to help the industry reach its full potential.

The interventions recommended here are still relatively light, and reflect the fact that cyber insurance is only a potential incentive for managing societal cyber risk. They include: developing guidance for minimum security standards for underwriting; expanding data collection and data sharing; mandating cyber insurance for government suppliers; and creating a new collaborative approach between insurers and intelligence and law enforcement agencies around ransomware.

Finally, although a well-functioning cyber insurance industry could improve cyber security practices on a societal scale, it is not a silver bullet for the cyber security challenge. It is important to remember that the primary purpose of cyber insurance is not to improve cyber security, but to transfer residual risk. As such, it should be one of many tools that governments and businesses can draw on to manage cyber risk more effectively.

Recommendations

THIS PAPER PROVIDES actionable recommendations for the UK cyber insurance market. Although they are specifically aimed at UK policymakers, regulators and insurance providers and brokers, they could potentially also be applied to other national contexts.

Recommendation 1: Insurers should collectively agree on a set of minimum security requirements as part of risk assessments for small and medium-sized enterprises (11–250 employees). In the UK, this paper recommends using the controls used for Cyber Essentials[3] as a minimum requirement, beyond which insurers can require additional controls based on claims data or other risk frameworks. This will help increase the baseline cyber security of many UK businesses.

Recommendation 2: Cyber insurance carriers should explore partnerships with managed security service providers, cloud service providers and threat intelligence providers to gain access to additional sources of data (for example, beyond only external perimeter scans). In exchange, insurers can offer reduced premiums and other financial incentives to their customers.

Recommendation 3: The insurance industry should take a more collegial approach to data sharing. The Treasury and the Department for Digital, Culture, Media and Sport (DCMS) should bring together relevant stakeholders, including relevant regulators, Lloyd's of London and the Association of British Insurers, to create a working group and identify a timeline for the creation of a cyber insurance data-sharing exchange.

Recommendation 4: The government and insurance regulators should review any current insurance regulation or legislation that impedes insurers collectively sharing data on cyber insurance incidents and claims, including confidentiality requirements in contracts. This effort can be led by the Treasury in the UK.

Recommendation 5: The government should ensure mandatory breach notification data is made available to the insurance industry. DCMS should work with the Information Commissioner's Office to find a compromise on providing anonymised breach data to the insurance industry. If one cannot be found, the government should amend the relevant legislation.

Recommendation 6: The government, underwriters and brokers should focus awareness and marketing campaigns around articulating and quantifying the financial costs of cyber risk to businesses and consumers.

Recommendation 7: The Cabinet Office and Crown Commercial Service should develop a policy and legal framework to mandate cyber insurance coverage for all government suppliers and

3. Cyber Essentials is a UK government-backed cyber security certification scheme.

vendors. This should specify minimum requirements and inclusions for coverage, whether coverage needs to vary by government department and a reasonable cover limit to ensure all affected organisations can access a policy.

Recommendation 8: The government should help organisations identify cyber insurance products that drive cyber security best practices. To do so, the National Cyber Security Centre (NCSC) should add more detailed guidance to its buyer's guide on services that may improve a policyholder's cyber security practices.

Recommendation 9: The Treasury, in coordination with the Bank of England and insurance industry stakeholders, should conduct a public study into the potential design and parameters of a government-backed financial backstop for cyber risk.

Recommendation 10: The National Security Secretariat should conduct an urgent policy review into the feasibility and suitability of banning ransom payments. The review should aim to produce actionable recommendations within three to six months and consult widely with relevant government departments, intelligence agencies, law enforcement and industry stakeholders. This should form part of a wider UK government review into policy options for combating ransomware.

Recommendation 11: The intelligence community, law enforcement and the insurance industry should establish a dedicated information-sharing partnership to exchange anonymised threat intelligence and incident response and cryptocurrency payment data relating to ransomware attacks. The NCSC, the National Crime Agency (NCA) and insurance industry stakeholders should leverage existing public–private partnership models for combating cyber threats and financial crime, such as the Joint Money Laundering Intelligence Taskforce.

Recommendation 12: Insurers should specify that any ransomware coverage must contain a requirement for policyholders to notify the NCA and the NCSC in the event of an attack and before a ransom is paid.

Recommendation 13: The insurance industry should work with the NCSC and cyber security partners to create a set of minimum ransomware controls based on threat intelligence and insurers' claims data. Insurance carriers should require these controls to be implemented as part of any ransomware coverage. These controls should include:

- Timely patching of critical vulnerabilities in external-facing IT infrastructure.
- Enabling multifactor authentication on remote-access services (such as remote desktop protocol instances).
- Limiting lateral movement by adopting network segmentation measures.
- Implementing procedures to ensure regular backups are created.[4]

4. James Sullivan and James Muir, 'Ransomware: A Perfect Storm', RUSI Emerging Insights, March 2021.

Introduction

CYBERCRIME IS THRIVING. One estimate puts global losses from cybercrime in 2020 at $945 billion,[1] while a recent report from the World Economic Forum highlights cybercrime as one of the most challenging risks facing societies in the next five years, alongside climate change and pandemics.[2] Although this trend predates the coronavirus pandemic, the spread of Covid-19 has emboldened cybercriminals. The threat posed by targeted ransomware operations, in particular, has increased in complexity and severity over the last 18 months.[3] Not only are the number of ransomware attacks increasing,[4] but the payments demanded by attackers are also increasing in value. One report suggests that from Q4 2019 to Q1 2021, the average ransom payment rose from $84,116 to $220,298.[5] It is clear that both critical national infrastructure (CNI)[6] and economic security are threatened by ransomware, and cybercrime more generally.[7] Meanwhile, governments and businesses continue to struggle to manage cyber risk.

---

1. Zhanna Malekos Smith and Eugenia Lostri, 'The Hidden Costs of Cybercrime', McAfee, December 2020, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>, accessed 23 March 2021.
2. World Economic Forum, *The Global Risks Report 2021: 16th Edition* (Cologny: World Economic Forum, 2021).
3. James Sullivan and James Muir, 'Ransomware: A Perfect Storm', RUSI Emerging Insights, March 2021.
4. Phil Muncaster, 'Ransomware Attacks Soared 150% in 2020', *Infosecurity Magazine*, 4 March 2021, <https://www.infosecurity-magazine.com/news/ransomware-attacks-soared-150-in/>, accessed 23 March 2021.
5. CoveWare, 'Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound', 26 April 2021, <https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound>, accessed 25 May 2021.
6. Ransomware groups have frequently targeted the healthcare sector, including hospitals involved in the coronavirus pandemic response. See Zack Whittaker, 'Healthcare Giant UHS Hit By Ransomware Attack, Sources Say', *TechCrunch*, 28 September 2020, <https://techcrunch.com/2020/09/28/universal-health-services-ransomware/>, accessed 23 March 2021.
7. A ransomware attack on the currency exchange provider Travelex was believed to be a major factor in the firm's collapse in August 2020. See Phil Muncaster, 'Travelex Forced into Administration After Ransomware Attack', *Infosecurity Magazine*, 10 August 2020, <https://www.infosecurity-magazine.com/news/travelex-forced-administration/>, accessed 23 March 2021.

Cyber insurance is one lever that could reduce the impact of cyber risk.[8] Although interest in its role is not new,[9] the growing impact of cyber risk has brought it to the forefront of government and business agendas. This is partly because cyber insurance enables organisations to transfer financial risk related to a cyber incident or attack. In addition, cyber insurers may be well placed to incentivise better cyber security practices as they can reward 'good' risk management, offer discounts in exchange for implementing security controls or standards, and provide cyber security services that some organisations may otherwise struggle to access. Cyber insurers may be uniquely placed to address cyber risk at scale as they have a financial incentive to reduce claims and losses.

Cyber insurance has also received a significant amount of negative media attention, particularly around the perceived non-payment of claims and its role in the ransomware epidemic.[10] The industry faces growing criticism that it is incentivising ransomware attacks by facilitating payments to organised cybercriminal groups, including those sanctioned by the US Treasury.[11] One notable intervention came in January 2021, when the former head of the UK's National Cyber Security Centre (NCSC) said that insurers were funding organised crime through ransom payments.[12] In addition, losses from ransomware are helping drive up premiums and even pushing some carriers to withdraw from the market.[13]

In light of this, this paper asks if cyber insurance can incentivise better cyber security practices and behaviours. It also addresses the key challenges facing the industry, including the potential negative effects that cyber insurance may have on cyber security. Furthermore, the paper identifies how the industry can overcome these challenges and champion the positive effects of cyber insurance.

The paper's findings and recommendations derive from a series of interviews and workshops. A previous RUSI Emerging Insights paper on cyber insurance highlighted some of the opportunities

8. Department for Digital, Culture, Media and Sport (DCMS), 'Cyber Security Incentives and Regulation Review 2020: Call for Evidence', 4 November 2019.
9. As outlined in Chapter I, academics and cyber security practitioners have been interested in the role of cyber insurance in improving cyber security practitioners since at least the late 1990s.
10. Renee Dudley, 'The Extortion Economy: How Insurance Companies Are Fueling 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 23 March 2021; Dan Sabbagh, 'Insurers "Funding Organised Crime" By Paying Ransomware Claims', *The Guardian*, 24 January 2021.
11. Andrew G Simpson, 'U.S. Treasury Warns Cyber Insurers Against Paying Ransomware Demands', *Insurance Journal*, 1 October 2020, <https://www.insurancejournal.com/news/national/2020/10/01/584906.htm>, accessed 6 November 2020.
12. Sabbagh, 'Insurers "Funding Organised Crime" By Paying Ransomware Claims'.
13. 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 25 May 2021.

and challenges for the industry,[14] and this follow-up paper seeks to broaden the evidence base on the relationship between cyber insurance and cyber security. In doing so, it provides actionable recommendations for policymakers and practitioners.

Structure

This paper is divided into four chapters. Chapter I outlines the purpose of cyber insurance and why some believe that it could improve cyber risk management practices. Chapter II presents primary research on the use of cyber insurance to improve cyber security. Chapter III assesses the challenges facing the cyber insurance industry. Chapter IV explores the levers that government and industry could pull to overcome these challenges and champion the positive effects of cyber insurance, drawing on potential 'lessons' from other types of insurance. The paper concludes with a set of targeted recommendations and suggestions for further research.

Methodology

This paper forms part of a 12-month research project conducted by RUSI and the University of Kent, entitled 'Incentivising Cybersecurity through Cyber Insurance'. It is funded by the UK's NCSC,[15] in collaboration with the Research Institute in Sociotechnical Cyber Security.[16] The project aims to explore ways in which cyber insurance could promote better cyber security practices. Specifically, it focuses on two questions:

- Can cyber insurance incentivise better cyber security practices and behaviours?
- If so, how can these positive impacts be better championed?

In answering these, the authors also consider whether cyber insurance can *negatively* affect cyber security.

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

- **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 53 semi-structured interviews with subject-matter experts from across the insurance and

14. James Sullivan and Jason R C Nurse, 'Cyber Security Incentives and the Role of Cyber Insurance', RUSI Emerging Insights, December 2020.
15. National Cyber Security Centre (NCSC), 'What We Do', <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>, accessed 23 March 2021.
16. Research Institute for Sociotechnical Cyber Security, 'About', <https://www.riscs.org.uk/about/>, accessed 23 March 2021.

cyber security industries, government, academia and potential purchasers of cyber insurance. Interview questions were formulated from the aforementioned research questions. 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 online between July 2020 and January 2021. 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,[17] which involved generating codes that reoccurred in interviews and identifying themes that provided insight into the research questions. Throughout this paper, an anonymised coding system based on Table 1 is used to refer to interview data in the footnotes.

- **Workshops**: The research team conducted two online workshops with key stakeholders from government, the insurance industry and business on 17 and 27 November 2020 under the Chatham House Rule.[18] Eight participants attended the first workshop, which was co-hosted by the World Economic Forum, and 31 participants joined the second. Attendees included a mix of interviewees and new participants, using the contacts established at the interviews. The workshops were used to validate and reassess themes identified in the literature review and interviews.

Table 1: Breakdown of Interviewees

Category	Type of Organisation	Count
Insurance industry	Cyber insurance (underwriters, brokers, reinsurers)	24
	Industry association	5
	Risk analytics	4
Business	Cyber security	7
	Financial services	3
	Consultancy	2
	Retail	1
	Legal advisory	1
Research	Academia	3
	Think tank	1
Government	Government	2
Total		**53**

Source: Author generated.

17. Virginia Braun and Victoria Clarke, 'Using Thematic Analysis in Psychology', *Qualitative Research in Psychology* (Vol. 3, No. 2, 2006), pp. 77–101.
18. Chatham House, 'Chatham House Rule', <https://www.chathamhouse.org/about-us/chatham-house-rule>, accessed 11 May 2021.

Limitations

There are two main limits to the generalisability of this paper's findings. First, the insurance market is cyclical and subject to pressure from wider economic forces. As most interviews were conducted in the second half of 2020, the latest round of insurance and reinsurance renewals in January 2021 may have impacted some of the market dynamics identified here. Second, findings may only be representative of the UK context, although it should be noted that many of the participants (especially cyber insurers) engaged in business internationally.

I. Cyber Insurance and the Cyber Security Challenge

DEDICATED CYBER INSURANCE policies first emerged in the 1990s to fill gaps in traditional insurance property and casualty products.[19] They grew as businesses became dependent on computer networks and the internet. Over the last two decades, cyber insurance products have evolved and offer a range of coverage. Although products lack standardisation, common features include: coverage for first- and third-party exposures; business interruption; third-party liabilities; data and software loss; cyber extortion; and regulatory notification costs.[20]

Cyber insurance has two primary purposes, depending on the needs of purchasers. The '101 definition' is that it provides a risk transfer mechanism. This enables an organisation to spread and defer financial risk to another party and cover at least some of the costs stemming from a cyber incident.[21] If used properly, this financial backstop serves as the last step in the risk management process. It emphasises that cyber insurance is intended to transfer *residual* risk – the risk that other cyber risk management practices cannot mitigate.[22] Put simply, cyber insurance policies aim to provide financial protection when all other cyber security measures have failed.

However, cyber insurance is also a services proposition. Interviews highlighted that some insurers and policymakers believe this to be the most valuable element of the cyber insurance offering.[23] At present, the most common type of services provided by cyber insurance products are 'post-incident'. They include forensic analysis, incident response, legal services and PR advice.[24] One cyber insurer described them as the 'blue lights of technology' as they are designed to help an organisation mitigate the worst effects of a cyber incident.[25] In the last few years, cyber insurance products have also started to include access to 'pre-incident services', which aim to

19. Mark Camillo, 'Cyber Risk and the Changing Role of Insurance', *Journal of Cyber Policy* (Vol. 2, No. 1, 2017), p. 53.
20. For a comprehensive list of the types of first- and third-party coverage provided by cyber insurance policies, see Cambridge Centre for Risk Studies and Risk Management Solutions, Inc., 'Managing Cyber Insurance Accumulation Risk', February 2016, <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf>, accessed 1 February 2020.
21. Association of British Insurers (ABI), 'Cyber Risk Insurance,' <https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/>, accessed 9 May 2021.
22. Authors' interview with Government 2, 7 January 2021.
23. Authors' interview with Government 1, 16 September 2020; authors' interview with Insurance Industry 7, 1 October 2020.
24. Sullivan and Nurse, 'Cyber Security Incentives and the Role of Cyber Insurance', p. 8.
25. Authors' interview with Insurance Industry 7, 1 October 2020.

prevent breaches and reduce the risk profile of the insured. These services are distinct from pre-breach security requirements, which insurers use to check a reasonable level of security is in place. Some examples of pre-incident services include training, attack surface monitoring and access to cyber security consulting.

It is also worth noting that cyber insurance is typically available in two distinct forms. It can be purchased as a standalone policy or as part of a general business insurance policy. The latter, known as a 'packaged' policy, is attractive for both simplicity and affordability, but may fail to provide extensive coverage, including comprehensive pre- and post-breach services.[26] Meanwhile, a standalone or dedicated cyber insurance policy deals solely with cyber risk. While it represents a more significant investment, it is also more likely to have higher coverage limits,[27] and offer access to post- and/or pre-breach services.[28]

Considering the variations in form, coverage, terms and services, the cyber insurance market is evolving and uncertain of its final destination.[29] One insurer stated that 'there's a debate within the wider insurance marketplace at the moment on what cyber insurance should be and do'.[30]

Cyber Insurance Uptake

It has been estimated that, as of early 2021, global cyber insurance premiums total approximately $5 billion.[31] However, available data on business uptake is limited and relies on industry surveys, which vary significantly in methodology and scope. These surveys consistently highlight that although cyber insurance uptake has increased in recent years, market growth has failed to meet expected rates.[32] This is certainly true of the UK market. The Department for Digital, Culture, Media and Sport's (DCMS) 'Cyber Security Breaches Survey 2021' estimates that approximately 6% of businesses have a specific cyber insurance policy, and 37% have cyber risk covered as part of a wider insurance policy. Uptake of standalone policies is also higher among large businesses

26. DCMS, 'Cyber Security Breaches Survey 2021', March 2021.
27. Authors' interview with Insurance Industry 4, 7 July 2020; Julie Bernard, 'Overcoming Challenges to Cyber Insurance Growth: Expanding Stand-Alone Policy Adoption Among Middle Market Business', Deloitte, 16 March 2020, <https://www2.deloitte.com/us/en/insights/industry/financial-services/cyber-insurance-market-growth.html>, accessed 9 November 2020.
28. Authors' interview with Insurance Industry 17, 17 August 2020; Cybersecurity and Infrastructure Security Agency (CISA), 'Cybersecurity Insurance', <https://www.cisa.gov/cybersecurity-insurance>, accessed 9 November 2020.
29. Xiaoying Xie, Charles Lee and Martin Eling, 'Cyber Insurance Offering and Performance: An Analysis of the U.S. Cyber Insurance Market', *Geneva Papers on Risk and Insurance – Issues and Practices* (Vol. 45, No. 4, 2020), pp. 690–736.
30. Authors' interview with Insurance Industry 5, 20 September 2020.
31. Tom Johansmeyer, 'Cybersecurity Insurance Has a Big Problem', *Harvard Business Review*, 11 January 2021.
32. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.

than small and medium-sized enterprises (SMEs) and micro businesses.[33] In the US, the market for cyber insurance is considerably larger and more mature than others due to the introduction of mandatory data breach notification laws in the 2000s and other regulatory drivers.[34] There is, however, still considerable room for growth and uptake remains low among SMEs.[35] Chapter III explores uptake issues in more detail.

Why Cyber Insurance?

Despite the patchy progress of the cyber insurance industry to date, interest in its potential role in improving cyber security has steadily grown. Academic research exploring the utility of cyber insurance and its potentially positive effects on cyber security practices spans at least two decades.[36] Governments and international institutions have also sought to emphasise its ability to improve cyber risk management on a societal level.[37] As one US law enforcement official underlined in a workshop, 'we've always thought the [insurance] industry is a great place to improve cyber security practices'.[38]

Historically, other types of insurance have played a role in reducing economic, environmental, technological and political risks. Although the primary purpose of insurance is to transfer risk, a by-product is that it can also improve safety and security in some cases. From setting up the first fire departments in the aftermath of the Great Fire of London to incentivising the use of seatbelts and airbags in the automotive industry, the insurance industry has sought to improve risk management practices for individuals and businesses.

Likewise, cyber insurance could be an important lever for improving cyber security. In the UK, public and private sector organisations continue to face informational, commercial and

33. DCMS, 'Cyber Security Breaches Survey 2021'.
34. The US market is estimated to make up approximately 70% of global cyber insurance premium. See S&P Global Ratings, 'Cyber Risk in a New Era: Insurers Can Be Part of the Solution', 2 February 2020, <https://www.spglobal.com/ratings/en/research/articles/200902-cyber-risk-in-a-new-era-insurers-can-be-part-of-the-solution-11590046>, accessed 23 March 2021. On the impact of US states' mandatory breach notification laws on cyber insurance uptake, see Jan Martin Lemnitzer, 'Why Cybersecurity Insurance Should Be Regulated and Compulsory', *Journal of Cyber Policy* (February 2021), p. 4.
35. Bethan Moorcraft, 'US Insurance Market Not Keeping Up With Cyber Risk Needs for Small Businesses', *Insurance Business*, 19 November 2020, <https://www.insurancebusinessmag.com/us/news/cyber/us-insurance-market-not-keeping-up-with-cyber-risk-needs-for-small-businesses-239608.aspx>, accessed 23 March 2021.
36. As noted by Daniel W Woods and Tyler Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', *Security and Privacy* (Vol. 18, No. 1, 2020), p. 22.
37. HM Government, 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk', March 2015; EU Agency for Network and Information Security (ENISA), *Cyber Insurance: Recent Advances, Good Practices and Challenges* (Heraklion: ENISA, 2016); OECD, *Enhancing the Role of Insurance in Cyber Risk Management* (Paris: OECD Publishing, 2017).
38. RUSI workshop, 17 November 2020.

technical barriers to effectively manage cyber risk.[39] SMEs and micro businesses are especially underprepared when it comes to cyber risk. For instance, a recent industry report found that 64% of surveyed businesses are 'novices' when it comes to cyber readiness.[40] The failure of many organisations – both large and small – to do the bare minimum in terms of cyber security and cyber hygiene has also been reiterated by the current spate of ransomware attacks, which exploit lax patch management processes and poorly authenticated remote access services.[41]

There is a solid body of theoretical arguments that cyber insurance could play a meaningful role in improving cyber security among businesses, as referenced in a previous RUSI Emerging Insights paper.[42] However, in practice, it is still yet to be seen if cyber insurance can fulfil this promise. Amid growing interest from policymakers, this paper aims to plug that gap.

39. DCMS, 'Cyber Security Incentives & Regulation Review: Summary of Responses to the Call for Evidence', 27 August 2020.
40. Hiscox, 'Hiscox Cyber Readiness Report 2020', June 2020, p. 10.
41. Catalin Cimpanu, 'Top Exploits Used By Ransomware Gangs Are VPN Bugs, But RDP Still Reigns Supreme', *ZDNet*, 24 August 2020, <https://www.zdnet.com/article/top-exploits-used-by-ransomware-gangs-are-vpn-bugs-but-rdp-still-reigns-supreme/>, accessed 23 March 2021.
42. Sullivan and Nurse, 'Cyber Security Incentives and the Role of Cyber Insurance'.

II. Unfulfilled Potential: The Role of Cyber Insurance in the Cyber Security Challenge

CYBER INSURANCE IS suffering from unfulfilled potential and currently has a limited impact on cyber security practices within businesses. This paper identifies evidence that while it has the potential to incentivise better cyber security practices within businesses, this is yet to fully materialise. Moreover, in the areas where cyber insurance does incentivise better cyber security practices, the effects are unevenly distributed across organisations. To some extent, the ability of cyber insurers to improve policyholders' cyber security appears to vary based on their levels of maturity. This means that the standard of underwriting and services varies significantly across providers, making it difficult for organisations and brokers to navigate the market.

Through a thematic analysis of the interview data, five ways by which cyber insurance has some positive effects on cyber security and risk management can be identified:

1. Assessing risk profiles and security practices.
2. Driving best practices.
3. Linking risk profiles and best practices to financial incentives.
4. Raising awareness of risk.
5. Providing access to services.

Further analysis of these effects draws on other empirical studies on cyber insurance.[43]

43. These include interview- or content-based analysis studies such as Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?'; 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); Sasha Romanosky et al., 'Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?', *Journal of Cyber Security* (Vol. 5, No. 1, 2019); ENISA, *Cyber Insurance*; ENISA, *Commonality of Risk Assessment Language in Cyber Insurance: Recommendations on Cyber Insurance* (Heraklion: ENISA, 2017).

Assessing Risk Profiles and Security Practices

To assess a client's risk profile, insurers can identify potential risks, poor cyber hygiene and bad practices via an initial risk assessment.[44] This process may encourage an organisation to assess their exposure to risk, implement new controls or remediate previously identified vulnerabilities.[45]

In most cases, an initial risk assessment involves a questionnaire or 'prop' form.[46] Within the cyber insurance industry, these forms try to query various information, including: the size and geography of the business; its sector; IT dependencies; security controls; training; data recovery measures; and incident history.[47] For larger companies, these assessments may also include tabletop exercises and on-site visits. In most cases, risk assessments take place on an annual basis during the renewals process.

While these assessments are designed to put a premium on an organisation's cyber risk, they may also highlight new risks, poor cyber hygiene or vulnerabilities. This may have particular value for SMEs, who may not have the expertise or processes to identify these risks in the first place.[48] Some insurers claim that this could lead to attempts to remediate these issues, or that organisations may raise their standards to perform better during the underwriting process.[49] In some circumstances, an organisation may be refused insurance if the cyber risk is rated too high, which could act as an incentive to improve practices for future assessments.[50]

One financial services provider suggested that there is some anecdotal evidence that questionnaires are now more specific – at least for larger businesses.[51] One cyber insurer also noted that over the last couple of years their firm's risk assessments have placed more emphasis on controls 'that have the biggest impact' and linked them to potential cyber threats specific to the policyholder. However, they were not able to provide evidence that this has had a positive effect on cyber security practices.[52]

---

44. Shauhin A Talesh, 'Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses', *Law and Social Inquiry* (Vol. 43, No. 2, 2018), pp. 417–40.
45. OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, p. 7.
46. A 'prop' or proposal form is a questionnaire that asks a series of queries to gather information about the organisation interested in purchasing a policy.
47. ENISA, *Cyber Insurance*, pp. 11–12; Nurse et al., 'The Data That Drives Cyber Insurance', pp. 3–4.
48. Authors' interview with Government 1, 16 September 2020.
49. Authors' interview with Insurance Industry 3, 7 October 2020; authors' interview with Insurance Industry 22, 20 October 2020.
50. One business noted that at least one insurer refused to insure them due to their high risk profile. Authors' interview with Large Business 4, 28 September 2020.
51. Authors' interview with Financial Services 3, 11 December 2020.
52. Authors' interview with Insurance Industry 3, 7 October 2020.

Risk assessments also increasingly employ first- or third-party external network scans to identify vulnerabilities, patching regularity, open ports and email security. In some cases, third-party providers will quantify the results and data from intelligence sources such as the dark web as a 'cyber risk rating score'. The extent to which these scores may inform a risk assessment is unclear.[53] One insurer suggested that scans allow both the insurance provider and the organisation to understand 'their cyber hygiene as a whole', emphasising the importance of these services to some insurers.[54] These scans are also useful because they mirror the approach taken by threat actors, who often scan for internet-facing vulnerabilities or ports to gain initial access to victims.

In theory, SMEs have more to gain from scanning services, as large businesses likely employ some form of network scanning, either in-house or via a third-party threat intelligence provider. There is some evidence that insurers using external scans have a quantifiable impact on mitigating some cyber threats. Corvus, a US insurer that has developed its own network scanning capability, reported that its scans for vulnerabilities and ports exploited by ransomware groups resulted in a 65% drop in ransomware-related claims from April to September 2020.[55] This is one example of cyber insurance having a tangible positive effect on cyber security practices.

At the same time, insurers, cyber security providers and businesses stressed that there are limitations with initial risk assessments. The experiences of one financial services provider suggest that the quality of risk assessments varies significantly by carrier.[56] One insurer indicated that some competitors 'don't even ask questions beyond a certain premium and that premium covers an awfully large amount of the market'.[57] Worryingly, the breadth and depth of risk assessments are often limited for smaller businesses.[58] A prop form for a micro business or SME might involve as few as four questions,[59] whereas underwriting a FTSE100 business will involve site visits, interviews and even examining hardware.[60] While this is in part because there is a higher level of risk being underwritten with a large business, it is also simply not cost effective to carry out in-depth assessments on smaller organisations. When underwriting SMEs, insurers often hope to cover as many as possible and rely on only a small number making claims.[61] In practice, this may mean cyber insurers are currently much less well positioned to influence the practices of SMEs during risk assessments.

53. Well-known providers that were mentioned in interviews include BitSight, SecurityScorecard and Cyence.
54. Authors' interview with Insurance Industry 6, 20 August 2020.
55. Lawrence Abrams, 'Cyber Insurer's Security Scans Reduced Ransomware Claims By 65%', *Bleeping Computer*, 22 September 2020, <https://www.bleepingcomputer.com/news/security/cyber-insurers-security-scans-reduced-ransomware-claims-by-65-percent/>, accessed 11 February 2021.
56. Authors' interview with Financial Services 3, 11 December 2020.
57. Authors' interview with Insurance Industry 20, 24 July 2020.
58. Nurse et al., 'The Data That Drives Cyber Insurance', p. 3.
59. Authors' interview with Cyber Security 4, 19 August 2020.
60. Authors' interview with Insurance Industry 22, 20 October 2020.
61. Authors' interview with Insurance Industry 1, 15 July 2020.

There are also questions around the type of information collected by insurers. One study of a cyber insurer's underwriting process highlighted that many forms prioritise questions on privacy (likely because of GDPR regulations), even though it is less relevant for sectors which do not store large amounts of personally identifiable information (PII), such as manufacturing.[62] More broadly, questions are often only linked to specific types of coverage and associated costs. A risk assessment may only relate to the costs covered by the policy and, as a consequence, give an incomplete picture of an organisation's risk profile and security practices.[63] Another question revolves around the extent to which technical security controls are assessed.[64] Businesses, insurers and cyber security providers all expressed misgivings about the ability of risk assessments to effectively measure an organisation's security posture based on the technical information currently collected.[65] For example, one insurance industry professional stated: 'Obviously we ask lots of questions and we come up with an underwriting rationale, but I think if we're absolutely honest with ourselves, we only scratch the surface as to that technical assessment'.[66]

Finally, while external network scanning tools and cyber risk rating services are useful capabilities for cyber insurers, they also have limitations – at least in their current form.[67] They provide an incomplete picture of a company's security practices given their focus on internet-facing IT infrastructure. As one cyber security practitioner emphasised, they do not account for cyber security practices related to internal practices or behaviours – potentially giving a misleading image of actual cyber risk.[68] External network scanners are also prone to producing false positives and false negatives,[69] which means underwriters may miscalculate an organisation's cyber risk. As a result, a policyholder may be financially punished through a premium based on incomplete or inaccurate data. The extent to which potential purchasers of cyber insurance are obligated to remediate software vulnerabilities or other risks identified by insurers' external scans is also unclear. While scans may increase awareness of potential risks, there is no strong evidence that they lead to actual change.

62. Nurse et al., 'The Data That Drives Cyber Insurance', p. 3.
63. *Ibid.*
64. Romanosky et al., 'Content Analysis of Cyber Insurance Policies'.
65. Authors' interview with Financial Services 2, 9 September 2020; authors' interview with Cyber Security 7, 22 September 2020; authors' interview with Insurance Industry 1, 15 July 2020.
66. Authors' interview with Insurance Industry 33, 29 July 2020.
67. Paul McKay, 'Cybersecurity Risk Ratings Market Outlook, 2020 and Beyond', Forrester, 16 March 2020, <https://www.riskrecon.com/forrester-report-2020-cybersecurity-ratings-market-outlook>, accessed 12 February 2021.
68. Cyber security practitioner, RUSI workshop, 27 November 2020.
69. *Recorded Future*, 'What You Need to Know About Vulnerability Scanners', 22 July 2020, <https://www.recordedfuture.com/vulnerability-scanner-definition/>, accessed 11 February 2021.

Driving Best Practices

The cyber insurance industry is well placed to drive best practices, as insurance carriers are financially motivated to reduce claims and losses.[70] This means that, in theory, there should be a 'push factor' from the insurance industry to raise standards and drive best practices.[71]

There are several ways in which this push factor may manifest itself. First, as insurers collect a significant pool of claims data, they can identify vulnerabilities which are being actively exploited by threat actors and recommend relevant security controls. In short, insurers can learn from failure at scale. One cyber insurer highlighted that after seeing their customers being targeted through a specific vulnerability, they could track 'the common point of failure, and then push this out to our insureds to help correct and fix the vulnerability before it impacts other insureds'.[72] However, both the extent to which organisations act on that advice and the extent to which they are contractually obligated to do so are unknown. Moreover, these activities appear to only be conducted by a small number of leading cyber insurers, meaning they do not capture the entire market.

Cyber insurers are also theoretically well placed to drive the adoption of reputable cyber security standards or frameworks like Cyber Essentials, ISO27001 or NIST.[73] This can happen in two ways: by requiring a potential purchaser of cyber insurance to be certified to a set of standards, or by drafting questionnaires that use them as a framework. Although some insurers expressed positive opinions about different security standards during interviews – particularly the ISO standards[74] and Cyber Essentials – there was no evidence to suggest that certification to a given set of standards is routinely a prerequisite for insurance. The evidence on how security standards inform questionnaires is also mixed. While many aspects of standards can be well represented, sometimes entire topics may be absent from forms.[75]

70. 'There's a strong incentive for insurance companies to try and get [their] customers to undertake those quite basic, cost-efficient things, to reduce that level of risk'. Authors' interview with Insurance Industry 5, 1 September 2020.
71. Authors' interview with Insurance Industry 27, 10 August 2020.
72. Authors' interview with Insurance Industry 3, 7 October 2020.
73. ISO, 'Popular Standards: ISO/IEC 27001 Information Security Management', <https://www.iso.org/isoiec-27001-information-security.html>, accessed 13 November 2020; NCSC, 'Cyber Essentials', <https://www.ncsc.gov.uk/cyberessentials/overview>, accessed 10 November 2020; National Institute of Standards and Technology (NIST), 'Cybersecurity Framework', <https://www.nist.gov/cyberframework>, accessed 10 November 2020.
74. Authors' interview with Insurance Industry 19, 15 July 2020; authors' interview with Insurance Industry 18, 18 August 2020.
75. Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms'; ENISA, *Commonality of Risk Assessment Language in Cyber Insurance*, pp. 26–27.

Much of the support insurance companies provide is the result of accumulated expertise, consolidated information and a network of security- and incident response-focused contacts.[76] This may mean that cyber insurers can act as 'orchestrators', managing different stakeholders and distributing expertise, services and guidance to policyholders.[77] However, it is not clear how this tangibly impacts an organisation's cyber security practices.

There are initiatives by insurers to identify services they deem effective. For instance, the Cyber Catalyst programme by Marsh brings together multiple insurers to evaluate cyber security products and define the ones most likely to have a positive effect on mitigating key cyber threats.[78] Allianz has also recently announced a partnership with the cyber security vendor Cisco that aims to mitigate the threat posed by ransomware.[79] While it is logical that insurers are well placed to assess the effectiveness of these products given their access to claims data, the extent to which businesses have acted on this guidance is unknown. Moreover, the possibility that recommendations may be driven by commercial interests and the relationship between insurer and security vendor, as much as the actual value and benefits of a service or product, cannot be discounted. The effectiveness of cyber security products is generally open to question, as security vendors have often found it difficult to demonstrate that they can reduce losses or the likelihood of attacks (especially considering that determined and well-resourced threat actors will most likely be successful).

While there is reason to believe that cyber insurance could drive best practice, it currently plays a limited role. This is particularly true at the SME level, where in some cases insurers appear to only ask a limited number of questions relating to security standards.[80]

There are also questions around the degree to which cyber insurers can influence the practices of large businesses. One financial services provider stressed that cyber insurance would never change their cyber security practices, as they trust their own best practices.[81] Another interviewee in the same sector reinforced this point by stating that they believed they were already following best practices.[82] This evidence is admittedly anecdotal, and the financial services sector already has stringent cyber security regulations. However, it highlights that cyber insurers face an uphill battle in convincing mature businesses that they can provide expertise on best practices.

76. Talesh, 'Data Breach, Privacy, and Cyber Insurance'.
77. S&P Global Ratings, 'Cyber Risk in a New Era'.
78. Marsh, 'Cyber Catalyst By Marsh', <https://www.marsh.com/us/campaigns/cyber-catalyst-by-marsh.html>, accessed 23 March 2021.
79. Allianz, 'Cisco, Apple, Aon, Allianz Introduce a First in Cyber Risk Management', 5 February 2018, <https://www.allianz.com/en/press/news/business/insurance/180205-allianz-cisco-apple-aon-cyber-risk-solution.html>, accessed 23 March 2021.
80. Authors' interview with Insurance Industry 12, 2 July 2020.
81. Authors' interview with Financial Services 1, 7 October 2020.
82. Authors' interview with Financial Services 2, 9 September 2020.

Linking Risk Profiles and Security Practices to Financial Incentives

The most powerful lever the insurance industry holds is arguably the ability to link an organisation's risk profile or cyber security practices to financial incentives such as reduced premiums, better terms and higher coverage. This should encourage adoption of best practices by offering a clear financial incentive.[83] Contracts may also contain security obligations that make claims payments conditional on the implementation of certain controls or best practices.[84]

In practice, several insurers suggested that organisations with good risk management or cyber security practices are rewarded.[85] In some cases, this was linked to the adoption of specific practices or services. For instance, one insurer provides an online cyber awareness platform for SMEs that reduces a buyer's excess if 80% of staff complete the training.[86] Another carrier also offers lower deductibles for ransomware attacks if organisations use Cisco's Ransomware Defense platform.[87]

This lever does appear to have some positive effects on businesses' approach to cyber risk management. One financial services provider emphasised that 'going through the process makes you want to ensure that you have gaps filled and that you are at a certain level so that you can get the best premium from the policy'.[88] Linking premiums and other financial incentives to risk levels and security practices means that cyber security staff can demonstrate return on investment for cyber security spending. As one chief information security officer (CISO) stated, the fact that their organisation's premiums have not gone up 'means I'm doing my job properly'.[89] In this way, cyber insurance could be an important lever for increasing boards' or senior management's awareness of cyber risk and the need for improved cyber security or risk management practices. As cyber risk is difficult to manage and quantify, boards often do not understand it and cyber security managers frequently struggle to communicate the severity of the problem or the need for increased investment.[90] However, boards *do* generally understand the value and purpose of insurance. After all, they have had to purchase professional indemnity, public liability and other lines for decades. As such, insurance dedicated to cyber risk may help ensure that cyber security, at least in part, is given the attention it deserves at board level and helps benchmark the performance of cyber risk management practices.

---

83. Jean Bolot and Marc LeLarge, 'Cyber Insurance as an Incentive for Internet Security', in M Eric Johnson (ed.), *Managing Information Risk and the Economics of Security* (New York, NY: Springer, 2009), pp. 269–90.
84. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 22.
85. Authors' interview with Insurance Industry 3, 7 October 2020; authors' interview with Insurance Industry 19, 15 July 2020; authors' interview with Insurance Industry 29, 30 July 2020.
86. See, for example, Hiscox, 'Knowledge is Power', <https://www.hiscox.co.uk/sites/uk/files/documents/2019-07/20116-CyberClear-Academy-flyer-2019.FINAL_.pdf>, accessed 1 March 2021.
87. See, for example, Allianz, 'Cisco, Apple, Aon, Allianz Introduce a First in Cyber Risk Management'.
88. Authors' interview with Financial Services 3, 11 December 2020.
89. Authors' interview with Retail 1, 28 September 2020.
90. Authors' interview with Government 2, 7 January 2021; authors' interview with Cyber Security 7, 22 September 2020.

However, there is little conclusive evidence that premium discounts or other financial incentives are directly improving organisations' cyber security practices.[91] In most cases, insurers provide financial discounts on the basis of a subjective assessment of an organisation's risk, rather than specific technical controls or security standards.[92] Indeed, one study found that 45% of pricing algorithms filed with US regulators did not even consider cyber security measures or controls.[93] It also appears that, in many cases, accreditation to a specific set of standards does not necessarily lead to a premium discount. One representative of an insurance industry body said of Cyber Essentials: 'When I've asked insurers "if a company does Cyber Essentials does that reduce the cost of their policy?", they say, "it's nice to have but it probably won't affect the price that the company will pay"'.[94]

Moreover, while insurers may provide discounts for organisations that take up recommended security products, there is no evidence that any are doing the same for the adoption of specific cyber security measures. While some offer discounts for controls already in place, one study emphasises this is different to offering premium discounts as an incentive for businesses to introduce new measures.[95] High-risk or immature businesses will need incentives to introduce proactive new measures, rather than receive rewards for retrospective action.

Finally, most insurers do not currently use contractual obligations to incentivise better cyber security practices.[96] Contracts could contain security obligations that make claims payments conditional on the implementation of security controls, but in practice insurers feel unable to decline claims or renew policies even in cases of negligence. According to several insurers, this is due to market pressures or to maintain relationships with customers.[97]

Increasing Awareness of Risk

Research for this paper revealed that cyber insurance facilitates greater thinking about risk among businesses.[98] It assists in raising awareness relating to poor cyber security, so that it is seen as a concrete threat to business. For example, insurers are well placed to emphasise the

91. 'You should reward the good risks and punish – not punish, but financially disadvantage – the bad risks, or even not insure them. That should in theory change it but in practice that's not happening'. Authors' interview with Insurance Industry 4, 7 July 2020.
92. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?'; Nurse et al., 'The Data That Drives Cyber Insurance', pp. 3–4.
93. Romanosky et al., 'Content Analysis of Cyber Insurance Policies'.
94. Authors' interview with Insurance Industry 1, 15 July 2020.
95. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?'.
96. Authors' interview with Insurance Industry 14, 13 July 2020; authors' interview with Insurance Industry 20, 24 July 2020.
97. *Ibid.*
98. Authors' interview with Financial Services 2, 9 September 2020; authors' interview with Financial Services 3, 11 December 2020; authors' interview with Retail 1, 28 September 2020.

potential financial impact of an incident. Cyber insurers can articulate specific cyber risk to a purchaser and help map strategies and processes to mitigate it.[99]

In some cases, insurers can identify areas of cyber risk that an organisation has not thought about before or given enough consideration. One large financial services provider, for instance, suggested that they spent considerably more time on their organisation's data loss prevention strategy after advice from an insurer.[100] In another interview, a CISO highlighted how an insurer identified a weakness in their data retention practices which 'we hadn't really recognised as that much of a risk'.[101] This illustrates how some insurers can bring a fresh perspective to an organisation's risk management practices,[102] and observe wider trends in the risk landscape that filter down to their customers.

On balance, increased risk awareness from cyber insurance may be confined to large businesses. Insurers have more time and resources to carry out thorough risk assessments for big accounts, involving site visits, detailed questionnaires, scenario-based exercises and more.[103] In contrast, risk assessments for SMEs can amount to just a few questions, which are unlikely to prompt serious internal reflection. This again emphasises that the benefits of cyber security practices may well by unevenly distributed.

Providing Access to Services

Many cyber insurers provide services to help organisations prevent breaches or to reduce the impact when they happen.

Post-Incident Services

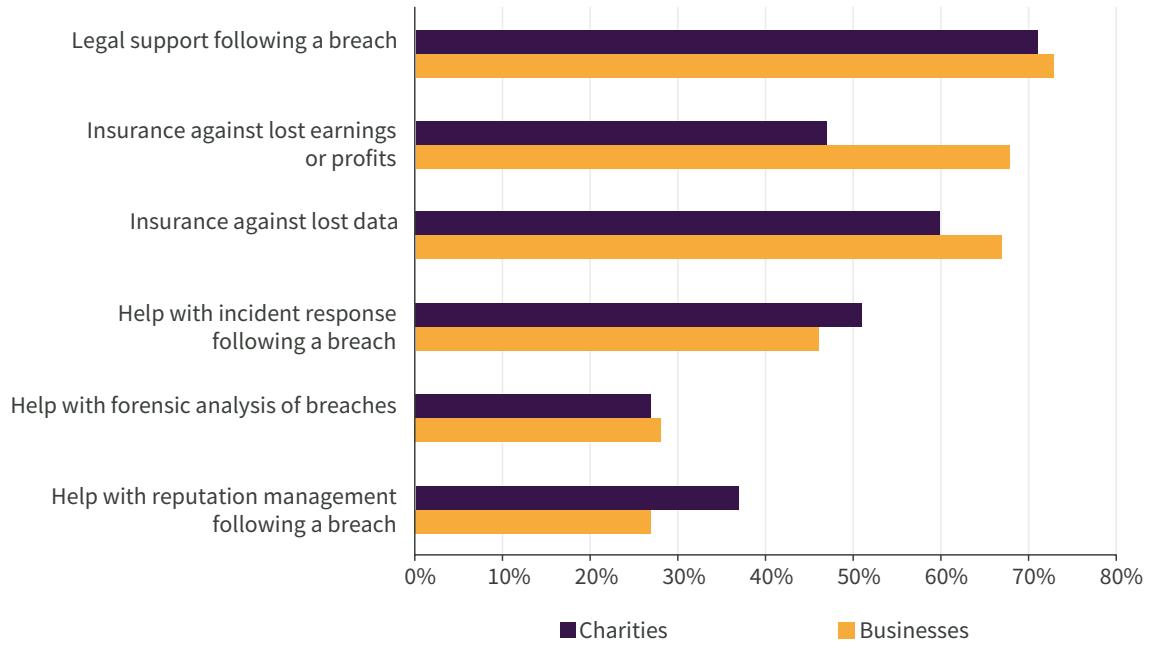
Post-incident services have become one of the success stories of cyber insurance for both insurers and insureds.[104] For insurers, they may reduce incident costs. For purchasers of cyber insurance – particularly SMEs – they provide access to services and expertise during crises.[105] Many interviewees noted post-breach services as one of the main benefits of cyber insurance, as they reduce losses and the impact of incidents. The most cited types of these services included incident response and forensics teams,[106] legal counsel[107] and, in some cases, PR specialists.[108]

99. Authors' interview with Academic 2, 30 July 2020; authors' interview with Consultancy 2, 1 October 2020; authors' interview with Retail 1, 28 September 2020.
100. Authors' interview with Financial Services 2, 9 September 2020.
101. Authors' interview with Retail 1, 28 September 2020.
102. Authors' interview with Financial Services 3, 11 December 2020.
103. Authors' interview with Consultancy 2, 1 October 2020.
104. Woods and Moore, 'Does Cyber Insurance Have a Future in Governing Cybersecurity?', p. 24.
105. Talesh, 'Data Breach, Privacy, and Cyber Insurance', p. 417.
106. Authors' interview with Insurance Industry 8, 7 September 2020.
107. Authors' interview with Insurance Industry 7, 1 October 2020.
108. Authors' interview with Insurance Industry 19, 14 July 2020.

The value of these services is deemed particularly important for SMEs, as they are less likely than large businesses to have in-house expertise or incident response providers on retainer.[109] Indeed, interviewees from large businesses emphasised they are less likely to use an insurer's post-incident services than their own.[110]

One risk is that some businesses – most likely micro and SMEs – do not have access to post-incident services in their cyber insurance policies. DCMS's 'Cyber Security Breaches Survey 2020' (Figure 1) suggests that most UK businesses surveyed do not have access to incident response (54% without coverage) or forensic analysis services (73% without coverage) as part of their coverage, although 73% do have access to legal support.[111] As a result, businesses that could gain the most from post-breach services may be less likely to have access to them. At the same time, it is important to acknowledge that this figure does cover organisations of all sizes, and some may intentionally choose not to include post-incident services in their coverage. Even so, this illustrates the lack of standardisation in coverage and how this may leave some policyholders with gaps.

Figure 1: Types of Coverage and Post-Breach Services Accessible by UK Businesses With Cyber Insurance



Source: DCMS, 'Cyber Security Breaches Survey 2020'.

109. Authors' interview with Insurance Industry 7, 1 October 2020; authors' interview with Government 1, 16 September 2020.
110. Authors' interview with Financial Services 1, 7 October 2020; authors' interview with Financial Services 2, 9 September 2020.
111. DCMS, 'Cyber Security Breaches Survey 2020'. The 2021 Cyber Security Breaches Survey did not ask respondents an equivalent question.

Although post-breach services do play an important role in reducing losses, they do not prevent incidents from happening in the first place. This means that they represent more of a responsive than preventative measure to improve cyber resilience. This was a frequent comment made by cyber security practitioners in interviews and workshops.

While cyber security is sometimes interpreted as a holistic process,[112] it is important to emphasise that post-incident services will not improve an organisation's ability to prevent incidents. That is not their intended purpose, and they should not be conflated with preventive controls or services.

Pre-Incident Services

Pre-incident services seek to proactively prevent incidents and mitigate risk. For specialist cyber insurance carriers, these services are increasingly a fundamental part of their offering in that they protect both insureds and their own loss ratios.[113] If appropriately targeted, pre-breach services could help organisations improve their cyber security practices and act as an additional incentive for purchasing cyber insurance. This is particularly true for SMEs, who are less likely to have access to these types of services or products.

112. NIST, 'Cybersecurity Framework'.
113. Cyber insurer, RUSI workshop, 27 November 2020.

Research for this paper identified a range of cyber risk management services, either free or discounted, as part of cyber insurance offerings. Solutions can be in-house or provided by a third-party vendor, and include:

- **Staff training**. This generally involves phishing-focused training.[114] For larger businesses, training may also include scenario-based tabletop exercises with senior management.[115]
- **Cyber risk rating services and vulnerability scanning**. Rather than using these tools as part of an initial risk assessment, some insurers use them off cycle to monitor internet-facing IT infrastructure or provide organisations with direct access to them.[116]
- **Threat intelligence services**. These types of services might involve deep and dark web monitoring to identify specific mentions of an organisation,[117] or using claims incidents to create security alerts or identify trends.[118]
- **Access to a virtual CISO**. This provides organisations without a senior cyber security manager with access to expertise.[119]
- **Password management solutions**.[120]

It is difficult to measure the effects of these services and tools, and several insurers highlighted that insureds are not using them at scale.[121] As one specialist cyber insurer noted, 'actually getting somebody to [use] something is still hard'.[122] Importantly, most insurance carriers are

114. CFC, 'Our Cyber Claims Service', <https://www.cfcunderwriting.com/media/3446/cfc-cyber-claims-brochure_digital.pdf>, accessed 5 March 2021; Chubb, 'Cyber Services', <https://www.chubb.com/uk-en/business/cyber-services.html>, accessed 5 March 2021; AIG, 'What's Inside CyberEdge', <https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Financial-lines/Cyber/cyberedge-2.0.pdf>, accessed 5 March 2021; QBE, 'Cyber Risk Management Services', 16 June 2020, <https://qbeeurope.com/document-library/risk-solutions/cyber-risk-management-services/>, accessed 5 March 2021; Beazley, 'Risk Management', <https://www.beazley.com/usa/cyber_and_executive_risk/cyber_and_tech/beazley_breach_response/cyber_services/risk_management.html>, accessed 5 March 2021.
115. Authors' interview with Insurance Industry 17, 17 August 2020; QBE, 'Cyber Risk Management Services'; AXIS, 'AXIS Cyber Tabletop Exercise', <https://www.axiscapital.com/insurance/cyber-technology-e-o/axis-cyber-services/prepare>, accessed 5 March 2021.
116. Authors' interview with Insurance Industry 14, 19 August 2020; authors' interview with Insurance Industry 3, 7 August 2020; CFC, 'Our Cyber Claims Service'; AIG, 'What's Inside CyberEdge'; QBE, 'Cyber Risk Management Services'.
117. CFC, 'Our Cyber Claims Service'; QBE, 'Cyber Risk Management Services'; AIG, 'What's Inside CyberEdge'.
118. Beazley, 'Risk Management'.
119. AIG, 'What's Inside CyberEdge'.
120. Chubb, 'Cyber Services'.
121. Authors' interview with Insurance Industry 20, 24 July 2020; authors' interview with Insurance Industry 14, 13 July 2020; authors' interview with Insurance Industry 7, 1 October 2020.
122. Authors' interview with Insurance Industry 14, 13 July 2020.

not linking pre-breach services to financial incentives (such as offering discounts in exchange for their use or denying claims if these services identify a risk which is not remediated).

There are also questions related to the effectiveness of these types of services. One insurer admitted that they are 'a lot more hit and miss' than post-breach services.[123] A survey of CISOs, executives and senior risk officers found that of the 28% of respondents that had used pre-breach services, only 48% said their needs were met.[124] At the same time, it is worth noting that the issue of efficacy is not unique to cyber insurers' preventive services. As highlighted in existing research, measuring and quantifying the value and effects of cyber security products is notoriously difficult and ultimately subjective.[125]

Pre-breach services are a significant development for cyber insurance. However, to be truly effective and incentivise good cyber security practices, insurers will need to refine them. At present, they lag behind post-breach services in terms of usability and impact.

Limitations of Cyber Insurance as an Incentive for Cyber Security

> 'I'm a little bit confused as to why it doesn't work as well as it should in theory'.[126]

Interviewees from across government, industry and business consistently stated that the positive effects of cyber insurance on cyber security have yet to fully materialise. While there are some encouraging signs, cyber insurance is still struggling to move from theory into practice when it comes to incentivising cyber security.

First, the positive effects of cyber insurance are not evenly distributed. It appears that some cyber insurers are offering products and services with a better chance at impacting security, reflecting insurers' varying level of maturity and expertise. Offerings are also not functioning as well as they might for SMEs and large businesses.

Second, in its current form, cyber insurance is more effective as a cyber *resilience* rather than *risk mitigation* tool. This is emphasised by the fact that post-breach services are the central cyber insurance service. This is not necessarily a criticism, as the main aim of cyber insurance is arguably to transfer residual risk and act as a last line of defence. The problem is that it

123. Authors' interview with Insurance Industry 7, 1 October 2020.
124. Advisen, 'Information Security and Cyber Risk Management', October 2020, p. 12, <https://f.hubspotusercontent20.net/hubfs/2558521/2020_ZurichCyberRMSurveyReport_v3.pdf?__hstc=185145974.8c72f2619c6115c433c9ce57b358ca07.1613321896391.1613321896391.1613321896391.1&__hssc=185145974.1.1613321896391&__hsfp=2218906227>, accessed 23 March 2021.
125. Ioannis Agrafiotis et al., 'The Relative Effectiveness of Widely Used Risk Controls and the Real Value of Compliance', Department of Computer Science, University of Oxford, November 2016, <https://www.cs.ox.ac.uk/files/8869/The_Relative_Effectiveness_of_widely_used_Risk_Controls_and_the_Real_Val....pdf>, accessed 23 March 2021.
126. Authors' interview with Government 2, 7 January 2021.

has yet to fully demonstrate that it can incentivise the proactive security practices that would make it more useful for managing cyber risk. Chapter III explores some of the reasons why this is yet to occur.

III. The Key Challenges

TO UNDERSTAND WHY cyber insurance has not fully realised its potential, this chapter outlines several challenges that may have impacted its effectiveness as a well-functioning incentive for better cyber security practices. These challenges were identified through a thematic analysis of interviews and existing literature. They include:

1. Negative dynamics in the cyber insurance market.
2. The lack of industry-wide minimum security standards and best practices.
3. The difficulties of collecting and modelling cyber risk data.
4. Concerns around the financial viability of the market.
5. Several longstanding barriers to uptake.
6. The potential for cyber insurance to incentivise negative behaviours related to the moral hazard and ransomware.

Challenge 1: Dynamics in the Cyber Insurance Market

> 'I don't know how constructive a role we're really playing. Because we've made it so easy to buy cyber insurance and it's just so cheap and so broad that there's neither carrot nor stick there'.[127]

An Immature Market

Cyber insurance is still in its infancy relative to other insurance lines. One interviewee said that this means that 'no one knows the right way to do it … a lot of things haven't been figured out'.[128] The result is that underwriters are going through a process of trial and error to understand how to assess cyber risk and the effectiveness of cyber security practices. The immaturity of the industry also manifests itself in levels of technical expertise. Cyber underwriting is still developing as a specialism, and the industry has also struggled to attract cyber security talent due to the competition for cyber security professionals and computer scientists.[129] Consequently, the cyber insurance market is not perceived – at least by some cyber security practitioners – to be a trusted partner.

127. Authors' interview with Insurance Industry 25, 3 September 2020.
128. Authors' interview with Insurance Industry 5, 1 September 2020.
129. Authors' interview with Insurance Industry 12, 2 July 2020; authors' interview with Insurance Industry 26, 3 September 2020. See also Ariel E Levite, Scott Kannry and Wyatt Hoffman, 'Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance', Research Report, Carnegie Endowment for International Peace, October 2018.

The 'Race to the Bottom'

In interviews, a number of insurers noted that the cyber insurance market has been characterised as 'soft' for much of the last two decades, with excess capacity and an influx of new insurers placing power in the hands of buyers and brokers.[130] Although there is roughly $5 billion in global cyber insurance premium, it is thinly spread across many different insurers, which creates competition for customers.[131] While competition can drive innovation and reduce costs for consumers, the cyber insurance market may be considered an example of the detrimental impact it can have. In this case, competition can be characterised as a 'race to the bottom', with some insurers arguably lowering underwriting requirements and standards to create 'less friction in the transaction'.[132]

In practice, the result is that cyber insurance providers may feel compelled to reduce security requirements and simplify questionnaires, making it harder to negotiate coverage that is conditional on accreditation to security standards or other best practices.[133] Underwriters that do try to insist on more stringent conditions or cyber hygiene clauses can find themselves undercut by competitors who are prepared to offer coverage without (or with fewer of) them.[134] This trend has been exacerbated by the actions of some brokers who, as one reinsurer argued, 'have been rigorous about making sure they have the broadest possible terms at the cheapest possible price with the least possible hassle'.[135] The race to the bottom has likely had a disproportionate impact on cyber insurers' ability to incentivise better cyber security practices at SME level, where the competition is particularly intense and underwriting practices are more lax.[136]

Fortunately, there are indications that this race to the bottom may be slowing and that the cyber insurance market is hardening.[137] Some insurers argue that the race ended in 2020.[138] There is certainly some anecdotal evidence to support this, with underwriters reportedly raising both premiums and underwriting standards.[139] This is partly driven by a broader hardening of the

130. Bethan Moorcraft, 'What is a Hard Insurance Market?', *Insurance Business*, 11 October 2019, <https://www.insurancebusinessmag.com/us/guides/what-is-a-hard-insurance-market-180382.aspx>, accessed 23 March 2021.
131. Johansmeyer, 'Cybersecurity Insurance Has a Big Problem'.
132. Authors' interview with Insurance Industry 14, 13 July 2020.
133. Nurse et al., 'The Data That Drives Cyber Insurance'; authors' interview with Insurance Industry 4, 7 July 2021.
134. Authors' interview with Government 2, 7 January 2021.
135. Authors' interview with Insurance Industry 25, 3 September 2020.
136. Authors' interview with Cyber Security 4, 19 August 2020.
137. Moorcraft, 'What is a Hard Insurance Market?'.
138. Authors' interview with Insurance Industry 9, 14 August 2020; authors' interview with Insurance Industry 30, 2 July 2020.
139. Erin Ayers, '"Sharp Pivots" in Cyber Insurance Market Keep Brokers Busy', Advisen, 1 February 2021, <https://www.advisen.com/tools/fpnproc/fpns/articles_new_1/P/388464595.html>, accessed 17 May 2021.

commercial insurance market following the economic fallout of the coronavirus pandemic,[140] but also because cyber insurers are grappling with rising losses. A recent industry report shows insured cyber losses of $1.8 billion in 2019, an increase of 50% year on year.[141] Ransomware has played a significant role in this trend and has emphasised that policyholders are not managing risk effectively.[142]

Consequently, cyber insurers may now (or very soon) be in a better position to improve insureds' cyber security practices and demand more rigorous security controls or other protective measures.[143] Losses may also drive less mature insurers with more lax underwriting standards out of the market. However, even if the financial incentives have changed owing to recent global events, the same issues outlined below around security standards and best practices, the use of data and lack of standardisation in coverage will persist. Moreover, a 'harder' market brings problems of its own and may mean that some businesses do not prioritise cyber insurance coverage due to the rising cost of insurance.

Challenge 2: Defining Best Practices and Minimum Standards

In contrast to more mature insurance lines like property, cyber insurance policies are not underwritten to standardised security requirements. This has limited the industry's ability to drive best cyber security practices by enabling the race to the bottom and pushing underwriters to rely on a subjective analysis of an organisation's cyber risk. In the absence of minimum security standards, potential purchasers of cyber insurance can simply choose a carrier that asks the fewest questions and requests less stringent security requirements.[144]

While the absence of industry-wide minimum standards is in part due to the immaturity and competitiveness of the cyber insurance market, this is not the only factor. Several insurers said that although there is some desire to band together on minimum standards, there are concerns that this would be viewed as anti-competitive by regulators. As a representative from a risk modelling service stated, 'I hate to think of the amount of things that I've been on

140. Katie Scott, 'Mactavish Warns That "Premiums Are Rising Dramatically" Due to Hardening Market', *Insurance Times*, 14 December 2020, <https://www.insurancetimes.co.uk/news/mactavish-warns-that-premiums-are-rising-dramatically-due-to-hardening-market/1435852.article?adredir=1>, accessed 18 February 2021.
141. Hiscox, 'Hiscox Cyber Readiness Report 2020', p. 7.
142. Catalin Cimpanu, 'Ransomware Accounted for 41% of All Cyber Insurance Claims in H1 2020', *ZDNet*, 10 September 2020, <https://www.zdnet.com/article/ransomware-accounts-to-41-of-all-cyber-insurance-claims/>, accessed 18 February 2021; Noor Zainab Hussain and Carolyn Cohn, 'Cyber Insurers Scale Back as Ransomware Attacks Rise', *Insurance Journal*, 17 December 2020, <https://www.insurancejournal.com/news/national/2020/12/17/594308.htm>, accessed 18 February 2021; authors' interview with Insurance Industry 30, 2 July 2020; authors' interview with Insurance Industry 32, 16 July 2020.
143. Ayers, '"Sharp Pivots" in Cyber Insurance Market Keep Brokers Busy'.
144. Authors' interview with Insurance Industry 30, 2 July 2020.

where someone has to read out an anti-trust notice at the start because insurers are terrified of anything deemed to be anti-trust'.[145]

However, even if those in the insurance industry were to come together to attempt to define and set minimum standards, there would still be significant questions as to what constitutes an adequate level of security and the most effective best practices. At present, according to participants from the insurance industry, government and academia, due to the lack of reliable cyber risk data, underwriters are still developing a robust evidence base for whether a particular security control leads to a measurable reduction in cyber risk.[146] While initiatives like Marsh's Cyber Catalyst are attempting to address this, it is still difficult to offer financial incentives in response for insureds implementing specific measures.

Policy papers on cyber insurance suggest using a range of possible frameworks and controls to set industry-wide minimum security standards, illustrating the ambiguity around best practices.[147] While government- or industry-led schemes such as Cyber Essentials, CIS 20,[148] NIST and the ISO standards share commonalities, controls also vary, especially with regard to the metrics used to measure success. Such controls are also only partly covered by cyber insurance proposal forms, which again points to the varied perspective of the market.[149] Regardless of how effective specific controls are,[150] there are also fears that they serve to emphasise compliance over secure behaviours and practices. Specifically, there are concerns that they act as box-ticking exercises which are easily gamed.[151] Indeed, some more mature sectors, such as financial services, are increasingly looking to a resilience-based rather than a compliance-based approach.[152]

145. Authors' interview with Insurance Industry 28, 27 July 2020.
146. Authors' interview with Academic 1, 27 July 2020; authors' interview with Insurance Industry 13, 21 July 2020; authors' interview with Government 2, 7 January 2021.
147. Daniel Woods and Andrew Simpson, 'Policy Measures and Cyber Insurance: A Framework', *Journal of Cyber Policy* (Vol. 2, No. 2, 2017), p. 218.
148. Center for Internet Security, 'The 20 CIS Controls & Resources', <https://www.cisecurity.org/controls/cis-controls-list/>, accessed 1 March 2021.
149. Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms'.
150. One survey suggests that businesses are split over their effectiveness in increasing cyber security. See Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey', Insights, September 2019, <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>, accessed 21 February 2021.
151. Authors' interview with Cyber Security 1, 18 September 2020.
152. A resilience-based framework involves stress-testing an organisation's cyber security and risk management practices based on penetration testing and scenarios. In the UK, one example of this is the Bank of England and Prudential Regulation Authority's CBEST scheme. For more details, see Bank of England, 'CBEST Threat Intelligence-Led Assessments', <https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity/cbest-threat-intelligence-led-assessments-implementation-guide>, accessed 7 May 2021.

The range of available security standards, technical controls and defensive cyber security products also emphasises that the challenge of measuring and implementing effective cyber security practices is not unique to the cyber insurance industry. As one policymaker noted, this is a problem also faced by governments and the cyber security industry, as the nature of cyber security is inherently unstable and subject to rapid change – 'you can never say this is what you have to implement and now you're secure, because the evolution of technology means that the only way you can truly be secure is to never use a computer'.[153]

While this challenge does not mean that insurers should give up trying to drive best practices, it does emphasise that any minimum security standards that government and industry set will only be baselines and subject to change.

Challenge 3: Collecting and Modelling Cyber Risk Data

The difficulties in assessing the effectiveness of cyber security standards and best practices point to a potentially more intractable challenge – the paucity and reliability of data. This means that cyber risk is hard to quantify, which in turn limits insurers' ability to accurately assess an organisation's risk profile or security practices and price policy premiums accordingly. As one insurer stated, 'we simply don't know what drives the losses'.[154] One result of this is that pricing is often based on one or a combination of market pressure, subjective judgement, or variables like a business's size or sector.

The Lack of Data

Part of this challenge relates to the lack of data: cyber attacks and other forms of malicious cyber activity are a relatively new phenomenon – at least compared to hurricanes or earthquakes – and there is still limited historical data on their financial impact. A 2018 survey by PwC, for instance, found that, on average, cyber insurance carriers only had seven years of claims data available to support underwriting and data modelling.[155] While this will now have increased, the lack of historical claims data remains a significant challenge for the industry.

This dynamic is not simply due to the immaturity of the cyber insurance industry. It is also a product of the lack of information sharing, both between insurers and policyholders and within the insurance industry. Insurers identify the lack of transparency from policyholders as an obstacle to collecting more accurate risk and claims data. Policyholders may, for instance, withhold information about cyber security practices, penetration testing results and past incidents from underwriters.[156] This can create an information asymmetry, where the risks are

153. Authors' interview with Government 2, 7 January 2021.
154. Authors' interview with Insurance Industry 27, 10 August 2020.
155. PwC, 'Are Insurers Adequately Balancing Risk & Opportunity? Findings from PwC's Global Cyber Insurance Survey', 2018, p. 3, <https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf>, accessed 22 February 2021.
156. OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, p. 96.

better understood by the insured than the insurer.[157] Organisations may be hesitant to reveal vulnerabilities that could harm their reputation or lead to them being targeted.[158] The latter is a legitimate concern, as cyber insurers have been caught up in well-publicised ransomware attacks where data has been leaked on the deep and dark web.[159] In some cases, the lack of information sharing between policyholders and insurers reflects the fact that personnel that engage with underwriters may simply not have oversight of or understand their organisation's IT assets and processes.[160] In very large organisations, even technical staff may not fully understand their exposure to cyber risk stemming from legacy IT infrastructure or third-party providers.

Although insurers could increase their pool of claims data by sharing it among themselves, the industry has so far proven resistant to this. This is largely because insurers see claims data as their intellectual property and the foundation of their competitive advantage. As one industry association representative emphasised, 'data is insurance – that's essentially what they make their money on'.[161] Previous studies have also highlighted that this is clearly an issue as the potential for an industry-wide pre-competitive cyber risk dataset was ruled out by insurers.[162] While this decision is understandable, the lack of an information-sharing mechanism between insurers continues to limit their collective ability to collect claims data in sufficient volume.

The Reliability of Data

A potentially more significant challenge is that even if more data was available to insurers, it may be unreliable due to the intangible, dynamic and systemic nature of cyber risk. This hinders efforts to quantify and model cyber risk for the purpose of pricing premiums and setting appropriate coverage.

First, estimating the potential impact of a cyber incident is difficult because many of the costs and harms are intangible – for example, reputational damage following a PII breach or the loss of intellectual property – and far-reaching. There are also a host of other harms which relate to physical, societal and physiological impacts of cyber attacks – these are extremely

157. CISA, 'Assessment of the Cyber Insurance Market', 21 December 2018, p. 9.
158. *Ibid.*
159. Lyle Adriano, 'Gallagher Hit By Ransomware Attack, Servers Disabled', *Insurance Business*, 30 September 2020, <https://www.insurancebusinessmag.com/uk/news/cyber/gallagher-hit-by-ransomware-attack-servers-disabled-234875.aspx>, accessed 1 March 2021; Phil Muncaster, 'Maze Authors Claim to Have Hit Insurer Chubb', *Infosecurity Magazine*, 30 March 2020, <https://www.infosecurity-magazine.com/news/maze-authors-claim-to-have-hit/>, accessed 23 March 2021.
160. CISA, 'Assessment of the Cyber Insurance Market', p. 10.
161. Authors' interview with Insurance Industry 1, 15 July 2020.
162. Nurse et al., 'The Data That Drives Cyber Insurance'.

difficult to estimate.[163] In the view of one underwriter, this means that 'it is subject to a lot more uncertainty, a lot more interpretation and a lot more subjectivity'.[164]

Second, cyber risk is dynamic. As one policy paper notes, the insurance industry has likely never faced a risk that can change so drastically.[165] The rapid evolution of digital technologies leads to new exposures and challenges that historical data may not be able to account for.[166] One insurer despaired that 'we've only got 10 [years of historical data] and actually nine of those are pretty useless because it's just moving so rapidly'.[167] Moreover, because cyber threats are anthropogenic, data has to account for threat actors constantly developing new tactics, techniques and procedures to bypass defensive cyber security measures. As such, the duration that data remains relevant for quantifying cyber risk and determining premiums may be shorter than historical data can account for. This is illustrated by the coronavirus pandemic, which has created significant changes both in the threat landscape and cyber security requirements due to the shift to remote working.

Finally, cyber risk is difficult to quantify as it has the potential to be systemic. Reliance on the same IT across different geographies and sectors means that a single event can have cascading effects that are difficult to model and predict.[168] Anticipating how systemic cyber risks might emerge can be particularly challenging because they can develop from a range of sources. As the examples of WannaCry,[169] NotPetya[170] and Microsoft Exchange[171] illustrate, exploitation of a widespread software vulnerability can impact businesses and organisations all around the world simultaneously. The potential for attacks on common technology service providers – for instance, a cloud service provider such as Amazon Web Services (which comprises 33% of global public cloud infrastructure) – could disrupt the operations of millions of insureds.[172] The systemic nature of cyber risk also raises the prospect of risk accumulation across different types

163. Ioannis Agrafiotis et al., 'A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate', *Journal of Cybersecurity* (Vol. 4, No. 1, 2018), pp. 1–15.
164. Authors' interview with Insurance Industry 13, 21 July 2020.
165. Levite, Kannry and Hoffman, 'Addressing the Private Sector Cybersecurity Predicament'.
166. OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, p. 95.
167. Authors' interview with Insurance Industry 13, 21 July 2020.
168. Lloyd's and University of Cambridge Centre for Risk Studies, 'Business Blackout', Emerging Risk Report, 2015, <https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloyds-business-blackout-scenario/>, accessed 1 March 2021.
169. Matthew Field, 'WannaCry Cyber Attack Cost the NHS £92 Million as 19,000 Appointments Cancelled', *The Telegraph*, 11 October 2018.
170. Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.
171. Brian Krebs, 'A Basic Timeline of the Exchange Mass-Hack', *Krebs on Security*, 8 March 2021, <https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/>, accessed 23 March 2021.
172. OECD, *Enhancing the Role of Cyber Insurance in Cyber Risk Management*, p. 97.

of coverage (such as property, business interruption and cyber) provided to a single insured.[173] This not only significantly complicates risk modelling and premium pricing, but also pushes insurers and reinsurers to lower financial limits in coverage.

Challenge 4: The Financial Viability of the Cyber Insurance Market

The inability to predict the effects of systemic risk has driven fears that a catastrophic incident could render insurers and reinsurers insolvent.[174] This is in part because, as one recent analysis put it, 'there just isn't enough money in cyber insurance'.[175] More specifically, there is arguably too little global premium to absorb losses from a systemic event. One effect of this is that insurers and reinsurers are also struggling to attract additional capital.[176]

This situation is partly a consequence of the race to the bottom, which has increased the market's financial exposure to systemic risk by driving down premiums and loosening underwriting.[177] As one insurance industry body representative illustrated:

> Particularly for smaller businesses, insurers are using laws of large numbers when it comes to assessing their risk. They're just betting on the fact that the loss from 10/15 of them is offset by the 200,000 of them that don't have a problem. The only problem is if you have something like NotPetya.[178]

Another contributory factor is what is known as 'silent cyber' coverage. This refers to insurance policies – normally property and casualty – which neither affirmatively cover nor specifically exclude cyber risks.[179] In practice, this exposes insurers to cyber risks that they have not collected premiums to cover. The potential consequences of silent cyber coverage were illustrated in the aftermath of the NotPetya attack, when pharmaceutical giant Merck and food and beverage producer Mondelez filed claims under their property and casualty insurance.[180] Silent cyber coverage can also open the door to 'double insurance' claims, whereby an insured claims on both its standalone cyber insurance policy and a silent cyber policy like property or business

173. Lincoln Kaffenberger and Emanuel Kopp, 'Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment', Carnegie Endowment for International Peace, 2019.
174. Authors' interview with Legal Advisory 1, 3 September 2020; Thomas Johansmeyer, 'Cyber Insurance Is Only a Few Claims Away From Disaster. This Is Why It Matters', World Economic Forum, 9 October 2020, <https://www.weforum.org/agenda/2020/10/there-s-not-enough-money-in-cyber-insurance/>, accessed 23 February 2021.
175. Johansmeyer, 'Cybersecurity Insurance Has a Big Problem'.
176. *Ibid.*
177. Authors' interview with Insurance Industry 27, 10 August 2020.
178. Authors' interview with Insurance Industry 1, 15 July 2020.
179. Jon Bateman, 'War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions', Carnegie Endowment for International Peace, 5 October 2020.
180. *Ibid.*

interruption.[181] This means that insurers may have no real idea of how financially exposed they are in the event of a systemic incident.

Finally, while challenges related to the financial viability of the cyber insurance market are normally associated with systemic risk stemming from a single incident or technological point of failure or vulnerability, the increasing frequency and severity of targeted ransomware operations has changed this calculation. Ransomware has driven cyber insurance losses over the last 18 months, and its impact 'cannot be overstated'.[182] This is because, unlike the majority of risks insurers cover, ransomware attacks are both a high-impact and a high-probability risk.

Challenge 5: Barriers to Increasing Uptake

As highlighted in Chapter I, cyber insurance uptake remains lower than expected, particularly among SMEs. Increasing market penetration remains a significant challenge for the industry. Even if insurers were able to champion the positive impact of cyber insurance more effectively, low uptake would still remain a significant barrier to doing so at scale. This challenge is driven by a combination of informational, commercial and trust-related barriers.

Lack of Understanding of Cyber Risk

In interviews, insurers and government officials consistently emphasised that organisations' failure to realise how vulnerable they are to cyber risks leads them to conclude that a cyber insurance policy is not cost effective. This applies much more to SMEs than large businesses and businesses in sectors with less cyber security regulation.

At first glance, this may be confusing. Surveys consistently suggest that awareness of cyber risk in businesses – even among SMEs – is increasing. For instance, in DCMS's 'Cyber Security Breaches Survey 2020', 80% of businesses suggested they view cyber security as a high priority (up from 69% in 2016).[183] However, there is still a widespread lack of understanding about its possible financial impact.

The intangible nature of cyber risk makes it difficult for potential purchasers to understand the value of cyber insurance.[184] Many understand it as a technical rather than an economic risk,[185] which can create a barrier to investing in cyber insurance due to the perceived absence of an obvious commercial rationale. A 2019 survey by Advisen found that 73% of brokers listed this as

181. Authors' interview with Legal Advisory 1, 3 September 2020.
182. Aon, 'Cyber Insurance Market Insights: Q3 2020', 2020, <https://aoninsights.com.au/wp-content/uploads/Cyber-Insurance-Market-Insights-Q3-2020.pdf>, accessed 23 February 2021.
183. DCMS, 'Cyber Security Breaches Survey 2020'.
184. Authors' interview with Insurance Industry 27, 10 August 2020; authors' interview with Insurance Industry 5, 1 September 2020.
185. Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey', p. 26.

the biggest obstacle to selling cyber insurance.[186] However, it is also worth noting that brokers might contribute to this issue as well, as some do not understand cyber risk themselves and are not able to articulate that there is an insurance product for it.

Organisations also find it hard to demonstrate a compelling case for investing in cyber insurance due to a misperception that threat actors only target certain sectors, large businesses or governments.[187] This creates, as one insurer put it, an 'it won't happen to me' syndrome that afflicts SMEs in particular.[188] Media reporting also tends to focus on incidents that affect large businesses or are of geopolitical significance, rather than cyber-enabled fraud or ransomware attacks against SMEs.

Prohibitive Costs

Another explanation for low uptake is the perceived high cost of standalone cyber insurance policies. Interviewees from the insurance industry highlighted that, in their experience, this was a particular problem for SMEs. Relative to other insurance policies, the cost of standalone policies can seem 'obscene' to them.[189] This has likely become more of an issue during the coronavirus pandemic, with budgets for discretionary spending on insurance reportedly significantly reduced.[190] In some cases, SMEs must now decide whether to buy insurance or keep their employees paid.[191] This factor has the potential to grow in significance as the insurance market hardens and premiums rise. A recent report by the Council of Insurance Agents and Brokers, for example, found that respondents reported an average premium increase for cyber insurance policies of 18% in Q1 2021.[192]

The barrier of prohibitive costs can be hard to square with the argument that, due to the race to the bottom, cyber insurance premiums have actually been lower than they should be relative to insurers' risk exposure. Indeed, one underwriter argued that premiums were at a 'price point which is close to the lowest they'll ever be' in 2020.[193] However, many organisations simply see cyber insurance as a luxury purchase rather than a necessity,[194] and this view serves to reinforce their purchasing decisions.

---

186. Advisen, 'Cyber Insurance – The Market's View', October 2019, p. 7, <https://www.advisenltd.com/2019-partner-re-survey-paper-cyber-insurance-the-markets-view/>, accessed 22 February 2021.
187. DCMS, 'Cyber Security Incentives & Regulation Review'.
188. Authors' interview with Insurance Industry 7, 1 October 2020.
189. Authors' interview with Insurance Industry 6, 20 August 2020.
190. Authors' interview with Insurance Industry 32, 16 July 2020; Bank of England, 'How Has Covid-19 Affected Small UK Companies?', 27 October 2020, <https://www.bankofengland.co.uk/bank-overground/2020/how-has-covid-19-affected-small-uk-companies>, accessed 22 February 2021.
191. Authors' interview with Insurance Industry 7, 1 October 2020.
192. Council of Insurance Agents and Brokers, 'Commercial Property/Casualty Market Index, Q1/2021', <https://www.ciab.com/resources/q1-p-c-markey-survey-2021/>, accessed 4 June 2021.
193. Authors' interview with Insurance Industry 14, 13 July 2020.
194. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.

Lack of Understanding of Cyber Insurance Products and Coverage

The difficulty of assessing the value of cyber insurance can be exacerbated by the lack of understanding about the types of incidents cyber insurance policies can cover. This is partly because cyber insurance coverage is not standardised, meaning there are significant differences in the types of coverage, exclusions and conditions found in different standalone policies.[195] Inconsistent terminology can make it very confusing for potential buyers – particularly SMEs – to compare different policies. Surveys of brokers, who play a significant role in helping buyers understand different types of coverage, highlight that they believe this lack of understanding is a significant obstacle to organisations buying standalone policies.[196] Again, however, this issue cuts both ways as some brokers may themselves not fully understand what cyber insurance products can offer.

In addition, many potential purchasers believe they are already covered by their existing property or liability policies.[197] While this may be a misunderstanding by purchasers in some cases, it may also be a result of brokers actively encouraging clients to expand existing property or liability policies rather than purchasing standalone cover.[198] This creates a significant challenge for insurers attempting to convince policyholders of the merits of standalone coverage and raises interesting questions about the broker–underwriter relationship.

Coverage is Too Limited and Restrictive

Some potential buyers believe cyber insurance coverage does not suit their needs. Interviewees identified this as the most significant barrier for large businesses purchasing cyber insurance. This is partly because financial limits are too low relative to some of their exposure.[199] As one financial services provider – albeit one with a standalone policy – stated, 'they're not giving you enough coverage for it to be adequate for the problem'.[200]

One insurer noted that many potential buyers are also worried about the breadth and depth of coverage.[201] The importance of this barrier to uptake may increase if, as some predict, cyber insurers try and exclude ransomware attacks from coverage.[202]

---

195. Authors' interview with Legal Advisory 1, 3 September 2020.
196. Advisen, 'Cyber Insurance – The Market's View', p. 7.
197. At least one survey lists this as the main obstacle to organisations purchasing standalone cover. See Bernard, 'Overcoming Challenges to Cyber Insurance Market Growth'.
198. OECD, *Enhancing the Role of Insurance in Cyber Risk Management*, p. 102.
199. Bernard, 'Overcoming Challenges to Cyber Insurance Market Growth'.
200. Authors' interview with Financial Services 2, 9 September 2020.
201. Authors' interview with Insurance Industry 29, 30 July 2020.
202. Mathew J Schwartz, 'As Ransomware Booms, Are Cyber Insurers Getting Cold Feet?', *BankInfoSecurity*, 8 December 2020, <https://www.bankinfosecurity.com/blogs/as-ransomware-booms-are-cyber-insurers-getting-cold-feet-p-2974>, accessed 22 February 2021.

Lack of Trust

Concerns around coverage feed into an important underlying factor: a lack of trust in cyber insurance. At least some businesses believe that cyber insurance will not pay out, or that it is an ineffective mechanism for managing risk. According to one cyber insurer, this belief is partly fed by a general distrust of the insurance industry.[203]

This trust gap has likely been exacerbated by the coronavirus pandemic, as demonstrated by a recent intervention by the UK's Financial Conduct Authority on behalf of thousands of companies seeking business interruption pay-outs that were refused by insurers.[204] Several interviewees also pointed to cynicism around cyber insurers following well-publicised claims disputes in the aftermath of the NotPetya attack as a limiting factor in uptake.[205] It should be noted that these criticisms are, to some extent, unfounded given the policies in question did not specifically include cyber insurance coverage.

These are not the only barriers to uptake. For instance, one common – and more general – refrain apparently heard at CISO level is that cyber insurance is simply 'not fit for purpose'.[206] In some cases, this viewpoint is not merely sceptical, but almost adversarial. This may be because some practitioners believe that the decision to purchase cyber insurance is an indictment of their own efforts, or that it will reduce or even replace investment in cyber security spending.

Challenge 6: Incentivising Negative Behaviours

There is a possibility that cyber insurance may be actively encouraging negative behaviours for both businesses and cybercriminals. In terms of businesses, the empirical evidence collected as part of this paper highlights that the moral hazard phenomenon is not occurring at scale with cyber insurance. However, cyber insurers may be unintentionally facilitating the behaviour of cybercriminals by contributing to the growth of targeted ransomware operations.

The Moral Hazard

> 'You wouldn't want your house to burn down because you have an insurance policy'.[207]

Some theoretical studies have argued that organisations are less likely to invest in risk prevention if they think that their cyber insurance policy will resolve (and/or cover the cost of) an incident

203. Authors' interview with Insurance Industry 4, 7 July 2020.
204. City of London, 'The Future of Cyber Insurance: Next Steps for the London Market', 2020, <https://www.theglobalcity.uk/resources/future-cyber-insurance>, accessed 22 February 2021.
205. Authors' interview with Retail 1, 28 September 2020; authors' interview with Insurance Industry 28, 27 July 2020; authors' interview with Insurance Industry 33, 29 July 2020.
206. Authors' interview with Insurance Industry 14, 13 July 2020; authors' interview with Insurance Industry 29, 30 July 2020.
207. Authors' interview with Insurance Industry 21, 17 September 2020.

anyway. This phenomenon is known as the 'moral hazard'.[208] For boards or senior management not inclined to defer to cyber security practitioners, cyber insurance could be viewed as a replacement for more costly cyber security measures.[209] If widespread, this could outweigh the potential positive benefits of cyber insurance by actively encouraging insecure practices and behaviours. It could also drive up insurance premiums, placing an increased financial burden on companies who do invest in cyber security and practice secure behaviours.[210]

However, research for this paper did not find strong empirical evidence indicating that the moral hazard is a significant issue for cyber insurance. While some insurers did suggest they had seen instances of businesses – particularly SMEs – treat cyber insurance as a substitute for increasing investment in cyber security,[211] most interviewees suggested that while the moral hazard could potentially occur, it is not often seen. This chimes with findings from DCMS's 'Cyber Security Breaches Survey 2019', which suggested that organisations consider cyber insurance as complementary to – rather than a substitute for – other forms of cyber risk management.[212]

This is primarily because cyber insurance policies do not cover *all* the potential impacts of cyber risk. For instance, financial coverage from a cyber insurance policy will not cover long-term reputational costs that can result from a data breach or ransomware attack, particularly if customer data is affected.[213] As one financial services provider stressed, 'there's no amount of cyber insurance pay-out that can remedy a severe loss of reputation'.[214] While this argument rests to some extent on the assumption that policyholders understand cyber risk, purchasers of cyber insurance do appear to have a greater understanding of the economic impacts of cyber incidents.[215] Moreover, the moral hazard issue may be attenuated by some of the scepticism around cyber insurance – specifically, that financial limits are too low to cover the costs of an incident and that organisations are not certain their policy will pay out.[216]

In sum, the moral hazard – as theoretically conceived – is not a significant challenge for the cyber insurance sector, at least no more so than it is for other insurance lines.

---

208. Kai-Lung Hui, Wendy Wan-Yee Hui and Wei Thoo Yue, 'Cyber Insurance and Risk Management: A Normative Analysis', 14 November 2019, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3486658>, accessed 10 September 2020.
209. Authors' interview with Insurance Industry 23, 14 August 2020.
210. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 26.
211. Authors' interview with Insurance Industry 15, 13 July 2020; authors' interview with Insurance Industry 17, 17 August 2020; authors' interview with Consultancy 1, 24 July 2020.
212. DCMS, 'Cyber Security Breaches Survey 2019', p. 25.
213. Authors' interview with Consultancy 2, 1 October 2020; authors' interview with Financial Services 3, 11 December 2020; authors' interview with Retail 1, 28 September 2020.
214. Authors' interview with Retail 1, 28 September 2020.
215. Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey', p. 30.
216. Authors' interview with Insurance Industry 14, 13 July 2020.

Cyber Insurance and Ransomware

The increasing impact of ransomware attacks has been a thread that runs through many of the challenges faced by the cyber insurance industry over the last couple of years. Targeted or 'human-operated' ransomware operations have driven up losses and premiums, and may lead to reductions in capacity and coverage. As outlined in a recent RUSI publication, the growing severity and frequency of targeted ransomware operations has been driven by several factors, including:

- A range of **initial access vectors** due to poor cyber security practices – particularly the exploitation of vulnerabilities in remote access services, which have grown in use during the coronavirus pandemic.
- The shift to **'double extortion' tactics**, which involves stealing as well as encrypting data.
- The growth of the **'ransomware-as-a-service' model**.
- A **permissive environment** for Russian cybercriminals.
- A **profitable business model** due to the normalisation of ransom payments and the professionalisation of ransomware operations.
- The use of **innovative marketing tactics**, including dedicated data leak sites, to increase pressure on victims.
- The use of **cryptocurrencies for ransom payments**, which are harder for governments and law enforcement to interdict.[217]

There are also widespread concerns that insurers are fuelling ransomware attacks by paying ransom demands. Paying ransoms is not currently illegal, and it is often cheaper to pay off extortionists than it is to rebuild IT infrastructure or cover losses from business interruption.[218] This, in turn, serves to normalise the act of making a payment, which has always been advised against by governments and law enforcement agencies.[219] It also adds fuel to the fire by incentivising more cybercriminals to engage in ransomware operations and enabling existing operators to invest in and expand their capabilities. A recent advisory by the US Department of the Treasury's Office of Foreign Assets Control also highlighted that cyber insurers may be facilitating payments to sanctioned individuals or entities.[220]

There is anecdotal evidence that insurers support paying ransoms, at least in some circumstances.[221] In interviews conducted for this paper, several insurers acknowledged that

217. Sullivan and Muir, 'Ransomware'.
218. Jan Lemnitzer, 'Ransomware Gangs Are Running Riot – Paying Them Off Doesn't Help', *The Conversation*, 17 February 2021, <https://theconversation.com/ransomware-gangs-are-running-riot-paying-them-off-doesnt-help-155254>, accessed 23 March 2021; Dudley, 'The Extortion Economy'.
219. Sullivan and Muir, 'Ransomware'.
220. US Department of the Treasury, 'Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments', 1 October 2020, <https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf>, accessed 22 February 2021.
221. Dudley, 'The Extortion Economy'.

they pay ransoms if alternatives are deemed unviable,[222] although one stressed that giving in to ransom demands is a 'last case scenario'.[223] Cybercriminals themselves appear to believe that victims with insurance are more likely to pay. In an interview with Talos Intelligence, a LockBit ransomware operator suggested that if a victim has a cyber insurance policy, a payment is 'all but guaranteed'.[224] Ransomware operators may therefore be actively targeting organisations with cyber insurance policies.[225] They can identify potential victims through open source intelligence gathering – for instance, insurers listing clients or public filings – or via initial reconnaissance on victims' networks. One threat intelligence provider highlighted at least one case where they had seen a ransomware operator steal copies of a victim's cyber insurance policy, before setting their ransom demand at the top end of the policy's financial limit.[226] This dynamic also makes cyber insurers an attractive target. In a recent interview, a member of the REvil ransomware group suggested that they are actively targeting insurers to steal information on policyholders.[227] The targeting of insurers also means that in some cases they are helping to normalise payments – in a prominent recent case, the insurer CNA paid a $40-million ransom to the operators of Hades ransomware.[228]

However, the role of cyber insurance in the ransomware epidemic is complicated. While it is logical that insurers may prefer to cover the lower costs of a ransom payment rather than a more expensive recovery process, the research for this paper has not found clear evidence that insurers are actively encouraging policyholders to choose the ransom payment option. Moreover, the incentives to pay are often strong, regardless of whether or not a victim has cyber insurance. In extreme cases, faced with potential bankruptcy or several weeks of downtime, many businesses will opt to pay irrespective of whether they have insurance policies. The Colonial Pipeline ransomware incident highlighted this dilemma for victims – although Colonial Pipeline had backups, the need to restore services swiftly pushed them to pay the ransom.[229]

222. Authors' interview with Insurance Industry 14, 13 July 2020; authors' interview with Insurance Industry 30, 2 July 2020.
223. Authors' interview with Insurance Industry 17, 17 August 2020.
224. Azim Khodjibaev, Dymtro Korzhevin and Kendall McKay, 'Interview with a LockBit Ransomware Operator', Talos, blog post, 2 February 2021, <https://blog.talosintelligence.com/2021/02/interview-with-lockbit-ransomware.html>, accessed 23 March 2021.
225. Samuel Greengard, 'The Double-Edged Sword of Cybersecurity Insurance', *Dark Reading*, 10 November 2020, <https://www.darkreading.com/edge/theedge/the-double-edged-sword-of-cybersecurity-insurance/b/d-id/1339412>, accessed 23 March 2021.
226. Authors' interview with Cyber Security 1, 20 September 2020.
227. 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 23 March 2021.
228. Kartikay Mehrotra and William Turton, 'CNA Financial Paid $40 Million in Ransom After March Cyberattack', *Bloomberg*, 20 May 2021.
229. Although it should also be noted that the decryption tool they were given by the ransomware operators did not work as effectively as promised, in turn emphasising why paying a ransom

These motivations can be even stronger in the public sector, where local governments, schools or hospitals may have to choose between disruption to essential services or paying a ransom. This highlights how the proliferation of ransomware attacks is a wider societal problem not limited to the role of cyber insurance.

In responding to this challenge, policymakers and cyber security practitioners should start from the premise that in the face of mounting losses and public criticism, insurers want – and need – a new approach.

should be avoided. See *BBC News*, 'Colonial Pipeline Boss Confirms $4.4 Million Ransom Payment', 19 May 2021.

IV. Helping the Cyber Insurance Industry Fulfil Its Potential

OVERCOMING THE KEY challenges and championing some of the positive effects outlined in Chapter II requires interventions and collaboration. While new approaches could draw on some lessons from the experiences of other insurance lines, the dynamic and systemic nature of cyber risk may limit their applicability.

The cyber insurance industry needs to come together on a more collegial basis, particularly around data sharing and minimum security standards. In addition, carriers need to move towards a more prescriptive risk management approach, whereby buyers are financially incentivised to adopt best practices. With the market undergoing changes amid growing losses, now is also the time for more coordinated action by government and regulators to help the industry reach its full potential as a tool for incentivising better cyber security practices.

Of the challenges revealed in Chapter III, the following are prioritised for recommendations:

- Defining minimum security standards and best practices.
- Increasing data collection and data sharing.
- Reducing barriers to uptake.
- Mitigating systemic risk.
- Ransomware.

While these recommendations primarily focus on the UK context, they have applicability in other national contexts as well.

Who Can Help Drive Positive Change?

Although the insurance industry, government and regulators have the biggest role to play, cyber insurance in the UK involves multiple stakeholders with various roles, responsibilities and capabilities (Figure 2). Solutions should draw on all of these parties where possible.

Figure 2: The UK Cyber Insurance Ecosystem

Source: Author generated.

Minimum Security Standards and Best Practices

The use of common standards and metrics in risk assessments would provide the insurance industry with more effective benchmarks for cyber security practices and ensure organisations – especially SMEs – receive more rigorous assessments. Research for this paper revealed that many in the insurance industry want more guidance from government on minimum security standards and best practices, but there is no agreement on how to approach this challenge.

A light-touch approach would be for more insurers to require certification to various sets of selected security standards or minimum security controls during the underwriting process, either as a prerequisite for insurance or in exchange for reduced premiums.[230] However, given this option has been available to insurers for some time and progress has been limited, it is not clear why the industry would suddenly embrace it without external pressure.

A more rigorous option for security would be for all insurers to use the same standardised minimum security requirements when assessing risk rather than relying on questions or controls based primarily on their claims data. However, a question remains about what minimum security requirements should be implemented and by whom.[231] So as not to confuse potential buyers, it is preferable to avoid a situation whereby insurers come up with an entirely new set of security requirements or best practices. Moreover, given that insurers have pre-existing commercial relationships with cyber security vendors, this may push them towards recommending certain controls or best practices for the wrong reasons.[232] Instead, this paper recommends that all insurers use Cyber Essentials as an existing baseline for assessing SMEs.[233] Although Cyber Essentials is sometimes criticised for being too basic, its simplicity is what makes it the best option for the UK. The controls required as part of Cyber Essentials would represent a *minimum* on top of which insurers can recommend additional controls or risk frameworks based on claims data or changes in the threat landscape. However, to account for the dynamic nature of cyber risk, the government and regulators are not yet in a position to mandate Cyber Essentials for cyber insurance policyholders.

Recommendation 1: Insurers should collectively agree on a set of minimum security requirements as part of risk assessments for SMEs (11–250 employees). In the UK, this paper recommends using the controls used for Cyber Essentials as a minimum requirement, beyond which insurers can require additional controls based on claims data or other risk frameworks. This will help increase the baseline cyber security of many UK businesses.

Data Collection and Risk Assessments

Rather than relying on expanding the depth of questionnaires or interviews to determine an organisation's cyber risk posture, underwriters could look to automated technical solutions to support long-term data-collection efforts. This could also allow for in-depth assessments of smaller organisations without the cost of intensive audits, which are arguably more justifiable with larger organisations.

230. Authors' interview with Insurance Industry 33, 29 July 2020.
231. Lemnitzer, 'Why Cybersecurity Insurance Should Be Regulated and Compulsory', p. 9; Woods and Simpson, 'Policy Measures and Cyber Insurance', p. 222.
232. Lemnitzer, 'Why Cybersecurity Insurance Should Be Regulated and Compulsory', p. 9.
233. This practice should not be applied to micro businesses, as the cost of becoming certified would be prohibitive.

Some insurers favoured expanding the use of external scanning or threat intelligence tools to increase data collection.[234] This approach could be refined by more insurers using claims data and threat intelligence feeds to identify vulnerabilities or weaknesses actively being exploited by threat actors. Insurers would then offer remediation advice on the most critical vulnerabilities to help policyholders reduce their risk. To drive positive change, underwriters could also make claims conditional on acting on this advice if a threat actor exploits a vulnerability identified by external scans. However, given the existing scepticism around insurers refusing claims, this may be a step too far.

As external scans only offer a partial view of an organisation's cyber security posture, a more effective approach might be to combine external scans with internal data sources.[235] In doing so, cyber insurance may be able to draw on car insurance, which sometimes uses a 'black box' in a policyholder's car to capture driver data, helping insurers set premiums based on driving behaviour. Although the success of this kind of car insurance is still up for debate,[236] it does emphasise a precedent for the use of telemetry in insurance. By monitoring the implementation of controls, anomalous network activity, cloud service configurations and other data points, insurers could assess risk in a much more data-driven fashion, monitoring changes in an organisation's risk posture. While some practitioners and policymakers highlighted potential drawbacks to this kind of monitoring[237] – for instance, false positives and an over-reliance on certain metrics – access to this type of feed would significantly increase the volume of data available to underwriters.

While insurance technology companies will almost certainly play a role in providing these kinds of capabilities in the future, in the short to medium term this 'black box' approach would likely require insurers to partner with existing suppliers or trusted partners. Interviews with business representatives highlighted the lack of trust around the idea of integrating insurers' hardware or software, given the implications for supply chain security and previous breaches of cyber insurers.[238] Instead, carriers should look to partner with providers already integrated into organisations' IT and security infrastructure, such as managed security service providers (MSSPs) and cloud services.[239] An advantage to this approach is that insurers gain insight into

234. Authors' interview with Insurance Industry 17, 17 August 2020; authors' interview with Insurance Industry 20, 24 July 2020.
235. Savino Dambra, Leyla Bilge and Davide Balzarotti, 'SoK: Cyber Insurance – Technical Challenges and a System Security Roadmap', <https://oaklandsok.github.io/papers/dambra2020.pdf>, accessed 3 January 2021.
236. Oliver Ralph, 'Drivers Put the Brakes on Car Insurance With a Black Box', *Financial Times*, 11 August 2017.
237. Authors' interview with Cyber Security 7, 22 September 2020; authors' interview with Government 2, 7 January 2021.
238. Authors' interview with Cyber Security 1, 18 September 2020; authors' interview with Financial Services 3, 11 December 2020.
239. For a recent example, see Phil Venables and Sunil Potti, 'Announcing the Risk Protection Program: Moving From Shared Responsibility to Shared Fate', Google Cloud, blog post, 2 March 2021,

potential sources of systemic risk and help to drive uptake. Other trusted partners that insurers could work with include law enforcement and national cyber security centres, as they are increasingly involved in monitoring and collecting data on cyber risk.

Recommendation 2: Cyber insurance carriers should explore partnerships with MSSPs, cloud service providers and threat intelligence providers to gain access to additional sources of data (for example, beyond only external perimeter scans). In exchange, insurers can offer reduced premiums and other financial incentives to their customers.

Data Sharing

Expanding the repository of threat intelligence, incident and claims data would also provide a stronger foundation for underwriting and modelling cyber risk.

Although governments and some elements of the insurance industry have been slow to act on data sharing, there has been progress in recent years. In the financial services and insurance industry, industry associations and non-profits such as ORIC International and ORX have increased the amount of operational risk data available to members. Some insurers are purchasing more information on cyber claims through private cyber risk management providers, such as Advisen.[240] Insurers themselves are also taking tentative steps towards sharing some of their own data. In the US, the for-profit Verisk Cyber Data Exchange aims to pool data among willing insurers on premiums, coverage and claims – although it is not clear how many have signed up.[241] A recent study with UK-based underwriters highlights the challenge with data sharing, with very little interest expressed in the creation of a shared pre-competitive dataset that would contain data central to insurance processes.[242] In the UK, insurers are also able to access the NCSC's Cyber Security Information Sharing Platform, which brings together industry and government partners to share cyber threat intelligence and vulnerability information.

However, governments, regulators and the insurance industry can go much further to improve data sharing. Stakeholders are currently pulling in different directions. Policy papers on cyber insurance suggest that governments and international institutions want insurers to embrace a more open-minded approach on sharing data among themselves,[243] while the insurance industry

<https://cloud.google.com/blog/products/identity-security/google-cloud-risk-protection-program-now-in-preview>, accessed 3 March 2021.

240. Advisen, 'Cyber Loss Data', <https://www.advisenltd.com/data/cyber-loss-data/>, accessed 4 March 2021.
241. Verisk, 'Cyber Data Exchange', <https://www.verisk.com/insurance/products/cyber-data-exchange/>, accessed 4 March 2021.
242. Nurse et al., 'The Data That Drives Cyber Insurance'.
243. US Cyberspace Solarium Commission, Final Report, March 2020, <https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view>, accessed 4 March 2021; OECD, 'Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation',

wants more access to governmental threat intelligence and breach notification data.[244] To move forward, governments and industry should meet in the middle. In the UK, the government should find a workable solution to the ABI's longstanding request to access anonymised GDPR breach data from the Information Commissioner's Office, in exchange for a firm commitment from large insurance carriers to agree to a claims data-sharing initiative.[245] While the value of GDPR breach data is, admittedly, of only limited value given that it primarily relates to incidents involving personal data, this would still be a useful incentive for collective action by insurers.

Recommendation 3: The insurance industry should take a more collegial approach to data sharing. The Treasury and DCMS should bring together relevant stakeholders, including relevant regulators, Lloyd's of London and the ABI, to create a working group and identify a timeline for the creation of a cyber insurance data-sharing exchange.

Recommendation 4: The government and insurance regulators should review any current insurance regulation or legislation that impedes insurers collectively sharing data on cyber insurance incidents and claims, including confidentiality requirements in contracts. This effort can be led by the Treasury in the UK.

Recommendation 5: The government should ensure mandatory breach notification data is made available to the insurance industry. The DCMS should work with the Information Commissioner's Office to find a compromise on providing anonymised breach data to the insurance industry. If one cannot be found, the government should amend the relevant legislation.

Overcoming Barriers to Uptake

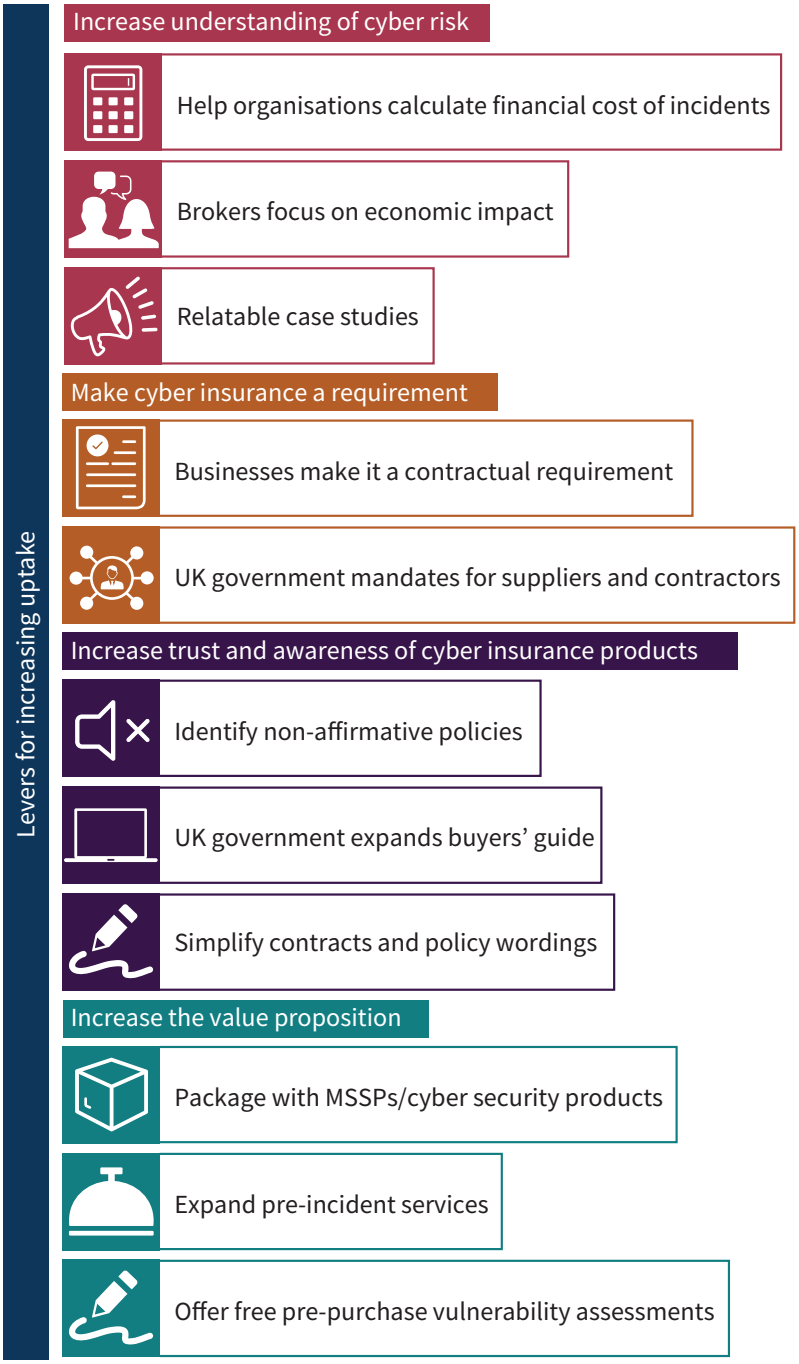
To spread the potential positive effects of cyber insurance on organisations' cyber security practices, governments and industry need to develop complementary efforts to drive uptake. Figure 3 illustrates a range of measures that could help achieve this.

2020, <https://www.oecd.org/daf/fin/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf>, accessed 4 March 2021; HM Government, 'UK Cyber Security'.

244. Authors' interview with Insurance Industry 4, 7 July 2020; authors' interview with Insurance Industry 1, 15 July 2020.

245. ABI, 'Speech: ABI Steps Up Call for Access to ICO Cyber Breach Data', 13 May 2019, <https://www.abi.org.uk/news/news-articles/2019/01/speech-abi-steps-up-call-for-access-to-ico-cyber-breach-data/?timeout=s>, accessed 7 January 2021.

Figure 3: Levers for Increasing Cyber Insurance Uptake



Source: Author generated.

Increasing Understanding of Cyber Risk

Organisations that assess the economic cost of cyber risk are much more likely to invest in both cyber security and cyber insurance. While awareness of cyber risk is likely to increase with time, future messaging on cyber risk and cyber security should reflect the fact that organisations want more relevant information on impact.[246] Despite the popular idea that cybercrime primarily affects large businesses, research suggests that in 2018 almost 63% of small UK businesses (understood as less than 50 employees) reported being a victim of cybercrime.[247] As such, campaigns on cybercrime should focus on tangible and relatable case studies. Given the key role of brokers in facilitating the purchase of insurance, the insurance industry should also focus on increasing their ability to articulate the importance of cyber security and the financial impact of cyber risk on buyers.

Recommendation 6: The government, underwriters and brokers should focus awareness and marketing campaigns around articulating and quantifying the financial costs of cyber risk to businesses and consumers.

Making Cyber Insurance a Requirement

A more drastic government intervention would make cyber insurance mandatory, putting it on the same statutory footing as professional liability insurance. This was supported in a recent research paper which suggested that the EU Commission or member states should announce their intention to make cyber insurance compulsory for SMEs over the next three to five years to drive uptake and increase societal resilience.[248]

While this kind of intervention would certainly dramatically increase uptake, it faces significant barriers. First, the market may simply be too immature for this kind of measure – not only in terms of its ability to absorb the capacity but also because cyber insurance products across the industry are still evolving. The market is still a long way from having the kind of standardised coverage that would be required. Moreover, even with the increasing digitalisation of the UK economy, it is not clear that all organisations, or particularly *every* SME, requires dedicated cyber insurance.

A more realistic alternative would be to develop approaches to increase uptake via vendor, regulatory or contractual requirements. Interviewees from the insurance industry and businesses suggested that contractual and vendor requirements are an increasingly significant factor in driving uptake, although this may be specific to certain sectors.[249] To drive this agenda

246. DCMS, 'Cyber Security Incentives & Regulation Review'.
247. Beaming, 'Small Businesses Hit Hardest By £17bn Cybercrime Bill in 2018', press release, 2019, <https://www.beaming.co.uk/press-releases/small-businesses-hit-hardest-by-17bn-cybercrime-bill-in-2018/>, accessed 4 March 2021.
248. Lemnitzer, 'Why Cybersecurity Insurance Should Be Regulated and Compulsory', p. 12.
249. Authors' interview with Insurance Industry 33, 29 July 2020; authors' interview with Financial Services 1, 7 October 2020.

forward, the UK government should use its procurement clout to ensure that all government contractors and suppliers require cyber insurance coverage, as they already do with Cyber Essentials certification.[250] This will allow the government to better manage cyber risk in its supply chain, but may also inspire regulators and businesses to follow suit over time.

Recommendation 7: The Cabinet Office and Crown Commercial Service should develop a policy and legal framework to mandate cyber insurance coverage for all government suppliers and vendors. This should specify minimum requirements and inclusions for coverage, whether coverage needs to vary by government department, and a reasonable cover limit to ensure all affected organisations can access a policy.

Increasing Trust and Awareness of Cyber Insurance Products

One possible approach to provide clarity on cyber insurance products could be for insurers – either with or without the intervention of industry regulators – to move towards standardising coverage and language.[251] This would allow buyers to more easily compare different insurers and have a firmer grasp of what their products include. However, now may not be the ideal time to standardise coverage given the current lack of reliable data on cyber risk and the need to innovate coverage to meet emerging threats. Instead, insurers should focus on simplifying wordings and contracts to help brokers and buyers navigate different offerings and remove barriers to trust.

Stakeholders could also seek to raise awareness about potential gaps or cyber exclusions in traditional property coverage. There are already moves in this direction in parts of the industry. In the UK, the Prudential Regulation Authority and Lloyd's of London have driven an agenda to identify silent cyber coverage. More clarity is now provided by either excluding or affirmatively covering the exposure from all property policies.[252] Future efforts could build on this initiative.

Governments can also play a role in increasing trust and awareness of cyber insurance products. To start, governments can more clearly articulate the potential value of cyber insurance to organisations. In the UK, DCMS should emphasise strengthening the role of cyber insurance in its next review of cyber security incentives and regulations. To accompany mandating cyber insurance for their suppliers, governments could also explore publishing buyer's guides or even creating certified suppliers to help organisations identify insurers that drive cyber security best practices. This could draw on previous government initiatives like the NCSC's list

250. Cabinet Office, 'Government Mandates New Cyber Security Standard for Suppliers', press release, 26 September 2014, <https://www.gov.uk/government/news/government-mandates-new-cyber-security-standard-for-suppliers>, accessed 4 March 2021.
251. ENISA, *Commonality of Risk Assessment Language in Cyber Insurance*.
252. Luke Gallin, 'Lloyd's Details Phased Implementation of Silent Cyber Mandate', *Reinsurance News*, 30 January 2020, <https://www.reinsurancene.ws/lloyds-details-phased-implementation-of-silent-cyber-mandate/>, accessed 5 March 2021.

of Cyber Assessment Framework-assured suppliers[253] or its certification scheme for training and degrees.[254] Although the NCSC has already produced a guide to cyber insurance,[255] several interviewees from the insurance industry argued that businesses still needed more detailed guidance or assurance.[256] Given the UK government may be unwilling to be involved in commercial product assurance, it could instead identify an independent body that could provide this service.

Recommendation 8: The government should help organisations identify cyber insurance products that also drive cyber security best practices. To do so, the NCSC should add more detailed guidance to its buyer's guide on services that may improve a policyholder's cyber security practices.

Increasing the Value Proposition

Given current losses and the general unavailability of reliable data to assess and price risk effectively, reducing premiums is not a viable option. While improvements in data collection and more accurate risk modelling may enable carriers to set prices at a more palatable rate over time, in the short to medium term insurers could also look to increase the value proposition of their offerings by expanding pre-incident services and other incentives. Carriers could also collaborate with brokers to offer potential buyers from the SME market free vulnerability assessments via automated external scans or cyber risk rating services to highlight their potential risks. Furthermore, insurers could look to partner with MSSPs or other cyber security vendors to package their policies with cyber security services and products.

Mitigating Systemic Cyber Risk

Insurers and reinsurers may be unable to address systemic or accumulated cyber risk on their own. More fundamentally, there is a good case to be made that governments should protect organisations from losses resulting from acts of war or terrorism.

To address this, the insurance industry, researchers and policymakers have increasingly explored the use of governmental backstop mechanisms to address cyber acts of war, terrorism and

253. NCSC, 'CAF Assured Products and Services', <https://www.ncsc.gov.uk/section/private-sector-cni/products-services>, accessed 4 June 2021.
254. NCSC, 'NCSC-Certified Degrees', 9 August 2017, <https://www.ncsc.gov.uk/information/ncsc-certified-degrees>, accessed 24 May 2021.
255. NCSC, 'Cyber Insurance Guidance', 6 August 2020, <https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance>, accessed 24 May 2021.
256. Authors' interview with Insurance Industry 8, 7 September 2020; authors' interview with Insurance Industry 19, 15 July 2020.

catastrophic incidents.[257] In the US, the Cyberspace Solarium Commission recently recommended a government study to explore what this would look like in practice.[258]

Existing proposals have investigated the possibility of replicating or expanding Pool Re in the UK, or the Terrorism Risk Insurance Act (TRIA) in the US. At present, both approaches have drawbacks. Pool Re is a private company that was founded in the aftermath of the Baltic Exchange bombing in 1992. It is a collective fund based on contributions from the insurance industry that is designed to cover all property claims resulting from terrorism above a certain amount. The UK government is liable for all losses exceeding 110% of the value of the fund.[259] However, some interviewees from the insurance industry suggested that 'Cyber Re' would be ill-suited to address cyber risk as the cost of a systemic cyber attack would likely far exceed the amount covered by the fund.[260]

An alternative is to build on the example of TRIA, a US governmental backstop created in the aftermath of the 9/11 attacks to prevent insurers withdrawing terrorism coverage. In this example, the government offers a guarantee to the insurance industry, albeit on its own terms as it has to certify an act of terrorism before the backstop pays out.[261] The limits of this mechanism have been illustrated by the US government's decision not to certify some incidents – notably the 2013 Boston bombing – as acts of terrorism.[262] This constraint would be even more significant in the context of cyber attacks, given the ambiguities around confidently attributing incidents to specific actors.

Approaches to creating governmental financial backstops clearly require further research and development. There are also still legitimate questions around whether taxpayers should pay for consequences of the private sector's poor cyber hygiene – NotPetya, for instance, was able to spread so rapidly due to slow patching.[263] With these issues in mind, governments should limit themselves to exploring the available options in more depth.

Recommendation 9: The Treasury, in coordination with the Bank of England and insurance industry stakeholders, should conduct a public study into the potential design and parameters of a government-backed financial backstop for cyber risk.

257. Bateman, 'War, Terrorism, and Catastrophe in Cyber Insurance'; Levite, Kannry and Hoffman, 'Addressing the Private Sector Cybersecurity Predicament'.
258. US Cyberspace Solarium Commission, Final Report, p. 82.
259. Woods and Simpson, 'Policy Measures and Cyber Insurance', p. 219.
260. Authors' interview with Insurance Industry 16, 20 August 2020.
261. Lemnitzer, 'Why Cyberscurity Insurance Should Be Regulated and Compulsory', p. 11.
262. *Insurance Journal*, 'Boston Bombing Lesson: Risk Managers Urge Better "Terror Act" Certification', 18 March 2015, <https://www.insurancejournal.com/news/national/2015/03/18/360930.htm>, accessed 5 March 2021.
263. Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History'.

Ransomware

Developing potential courses of action for mitigating the threat posed by ransomware has become a significant challenge for businesses, policymakers, law enforcement and national cyber security agencies. A recent report by the Ransomware Task Force laid out a policy framework for combating ransomware.[264] Although as the report highlights that a whole-of-government response is necessary for ransomware, this paper focuses primarily on measures that relate to cyber insurance. Specifically, the cyber insurance industry may be able to play a role in disrupting the ransomware business model, improving policyholders' defences against the threat, and supporting law enforcement action and even offensive cyber operations against ransomware groups.

To date, most of the existing debate has revolved around the feasibility and suitability of banning ransom payments.[265] In January 2021, the former head of the UK's NCSC suggested that 'you have to look seriously about changing the law on insurance and banning these payments'.[266] In essence, by removing the ability of ransomware groups to profit from their attacks, policymakers can discourage the business model driving the growth of ransomware. Policymakers – in consultation with industry – should explore this option seriously, but it by no means represents an easy fix and could have a variety of unintended consequences. As opponents of a ban have suggested, some victims would likely pay regardless, driving the process underground and making it even more difficult to track incidents.[267] Criminalising payments would also likely require some sort of exemption for certain critical national infrastructure providers to maintain essential services, such as healthcare or energy providers. However, given ransomware operators have been tenacious in selecting victims to maximise returns, this could serve to incentivise attacks against these sectors.

An alternative would be for insurers – either individually or collectively in consultation with government and regulators – to withdraw coverage for ransom payments while retaining coverage for the costs of recovering from an attack, as AXA France did in May 2021.[268] This may push more policyholders to choose recovery rather than pay a ransom. However, the impact of this on ransomware operations may be more limited than some hope, given that one of the strongest incentives to pay – the need to maintain services – will still be strong for many victims. Moreover, given that the majority of organisations – at least outside the US – still do not have cyber insurance coverage, it would likely not affect many ransomware victims. Given the strong arguments for and against banning ransom payments and the increasing importance of the

264. A coalition of stakeholders from across industry, government, law enforcement and international organisations. See also Sullivan and Muir, 'Ransomware'.
265. Alex Scroxton, 'Is It Time to Ban Ransomware Insurance Payments?', *Computer Weekly*, 11 February 2021, <https://www.computerweekly.com/feature/Is-it-time-to-ban-ransomware-insurance-payments>, accessed 6 March 2021.
266. Dan Sabbagh, 'Insurers "Funding Organised Crime" By Paying Ransomware Claims'.
267. Joe Tidy, 'Ransomware: Should Paying Hacker Ransoms Be Illegal?', *BBC News*, 20 May 2021.
268. Frank Bajak, 'Insurer AXA Halts Ransomware Crime Reimbursement in France', *AP News*, 6 May 2021.

ransomware epidemic to national security and the economy, the government should conduct an urgent policy review on the subject.

Policymakers should also look beyond the issue of banning ransom payments. Government and law enforcement should collaborate with the insurance industry to prevent attacks from occurring in the first place and pursue the criminals that carry them out. Insurers should collectively coordinate with the NCSC to drive best practices among policyholders (for instance, identifying controls to mitigate against known ransomware tactics and creating corresponding security obligations in ransomware coverage). One insurer suggested that there could be support for this measure within the industry.[269]

These measures could represent the basis of a broader effort to coordinate and share intelligence on ransomware. The government needs to elevate the importance of ransomware with national security, intelligence and law enforcement agencies. Insurers collect considerable amounts of data on ransomware events, ranging from the sectors that are most likely to be attacked and the size of ransom demands to information on specific cryptocurrency wallets used by ransomware groups.[270] This could provide investigatory teams seeking to establish operators' identities and disrupt technical activity with more relevant data. Media reporting suggests that this kind of collaboration is already occurring in the US informally.[271] Relevant stakeholders in the UK could seek to expand and formalise this practice. In the short term, government and regulators should move quickly to pressure insurers to create contractual obligations that ensure that policyholders notify law enforcement immediately after an attack and before a ransom payment is made.[272] The government should also explore legislation for mandatory reporting of ransomware payments to a designated authority as part of the review into ransom payments.

Recommendation 10: The National Security Secretariat should conduct an urgent policy review into the feasibility and suitability of banning ransom payments. The review should aim to produce actionable recommendations within three to six months and consult widely with relevant government departments, intelligence agencies, law enforcement and industry stakeholders. This should form part of a wider UK government review into policy options for combating ransomware.

Recommendation 11: The intelligence community, law enforcement and the insurance industry should establish a dedicated information-sharing partnership to exchange anonymised threat intelligence and incident response and cryptocurrency payment data relating to ransomware attacks. The NCSC, the NCA and insurance industry stakeholders should leverage existing

269. Authors' interview with Insurance Industry 17, 17 August 2020.
270. Jeff Stone, 'FBI Turns to Insurers to Grasp the Full Reach of Ransomware', *CyberScoop*, 30 March 2020, <https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/>, accessed 5 March 2021.
271. *Ibid.*
272. New York State Department of Financial Services, 'Insurance Circular Letter No. 2 (2021)', 4 February 2021, <https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02#_edn10>, accessed 5 March 2021.

public–private partnership models for combating cyber threats and financial crime, such as the Joint Money Laundering Intelligence Taskforce.

Recommendation 12: Insurers should specify that any ransomware coverage must contain a requirement for policyholders to notify the NCSC and the NCA in the event of an attack and before a ransom is paid.

Recommendation 13: The insurance industry should work with the NCSC and cyber security partners to create a set of minimum ransomware controls based on threat intelligence and insurers' claims data. Insurance carriers should require these controls to be implemented as part of any ransomware coverage. These controls should include:

- Timely patching of critical vulnerabilities in external-facing IT infrastructure.
- Enabling multifactor authentication on remote-access services (such as remote desktop protocol instances).
- Limiting lateral movement by adopting network segmentation measures.
- Implementing procedures to ensure regular backups are created.[273]

273. Sullivan and Muir, 'Ransomware'.

Conclusions

CYBER RISK POSES a complicated and growing challenge for governments, businesses and consumers. This paper explores cyber insurance's potential contribution to solving this problem. To date, the shortcomings of cyber insurance mean that its impact is ultimately more limited than policymakers and businesses might hope. Most of the cyber insurance market has used neither carrots (financial incentives) nor sticks (security obligations) to improve the cyber security practices of policyholders. However, growing losses have also emphasised that the current reality is not sustainable for insurers either.

The industry is also beset by an array of challenges that have limited the effectiveness and growth of cyber insurance products. Perhaps most fundamental is the lack of understanding around what drives losses and the kind of cyber security practices and products that prevent them. To overcome this and other challenges facing the industry, this paper identifies a number of interventions for the insurance industry and policymakers. Ultimately, these efforts need to be complementary and coordinated to succeed. New approaches to improving minimum security standards, sharing data and combating ransomware demonstrate that this process is not only collaborative but also iterative. Government and the insurance industry each have access to a range of data sources that can improve best practices. A well-functioning and more collegial insurance industry can help law enforcement and national cyber security centres identify threats that are active within a particular industry or sector.

It is also important to temper expectations. Even if cyber insurance functions as many would hope, it is still not a silver bullet for managing societal cyber risk. It is just one lever that policymakers and the private sector can draw on to incentivise better cyber security practices. Moreover, the purpose of cyber insurance – which is ultimately about transferring residual risk – should be remembered. If insurance can improve cyber security practices, this is a by-product rather than its core purpose.

Further research is needed on several issues identified in this paper, including:

- The effectiveness of pre-incident services provided by cyber insurers, and how these can be better integrated with post-breach service offerings.
- Vendors or products that occur commonly in pre- and post-incident services provided by cyber insurers. These may also introduce some central area of risk.
- The extent to which cyber risk is unique compared to other types of risk covered by insurance.
- The experiences of other insurance lines in developing minimum security or safety standards.
- The potential role of telematics (for instance, how can insurers model risk from network monitoring services which produce a high number of false positives?).

- To what extent has the cyber insurance contributed to the growth of ransomware?
- To what extent are insurers a target for ransomware groups?
- How can the insurance industry and government learn from the experiences of banning some types of kidnap and ransom payments, for instance to terrorist organisations or organised crime groups?

The impact of ransomware on the cyber insurance industry emphasises the need to address some of these issues and questions sooner rather than later. As some insurers risk being overwhelmed by losses, the industry and governments need to react quickly to ensure adequate protection and coverage for businesses.

About the Authors

Jamie MacColl is a Research Analyst 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 cyber insurance and cyber risks related to the globalisation of technology.

Jason R C Nurse is an Associate Professor in Cyber Security at the University of Kent and a core member of the Institute of Cyber Security for Society (iCSS). He is also a RUSI Associate Fellow, a Visiting Academic at the University of Oxford, and a Visiting Fellow in Defence and Security at Cranfield University. His research focuses on cyber security as an interdisciplinary problem, and he currently explores topics such as cyber insurance, corporate communications relating to security, and cybercrime.

James Sullivan is Director of Cyber Research at RUSI. His research focuses on national cyber strategies, the globalisation of technology, cyber resilience, cybercrime and issues relating to offensive cyber.