RUSI
www.rusi.org
Royal United Services Institute
for Defence and Security Studies

University of Kent

EMERGING INSIGHTS

Cyber Security Incentives and the Role of Cyber Insurance

James Sullivan and Jason R C Nurse

EXECUTIVE SUMMARY

- This paper outlines the opportunities of and challenges in using cyber insurance to incentivise cyber security practices. Findings are based on a review of existing industry reports and academic research.
- The paper forms part of an independent research project by RUSI and the University of Kent that provides actionable policy recommendations on how to incentivise cyber security through cyber insurance. They derive from a series of interviews and workshops with insurers, businesses, cyber security providers, government and other key stakeholders.
- The current evidence about the ability of cyber insurance to improve cyber security practices is limited. While cyber insurers may be able to provide expertise to policyholders and increase their awareness of cyber risks, much of the existing evidence base is largely theoretical and there is still considerable scepticism from customers about the benefits of cyber insurance.
- The uptake of cyber insurance, particularly by small to medium enterprises (SMEs), remains low. Existing research suggests that some of the overarching factors explaining this are: the high cost of policies and the difficulties insurers face in pricing premiums appropriately; confusion over what types of incidents insurance policies cover (and the issue of 'silent cyber'); and a lack of understanding of risks stemming from cyber incidents.
- There is the potential for the cyber insurance market to learn from other insurance markets to increase uptake, although understanding the depth of these connections requires further enquiry.
- The paper concludes by identifying several policy questions raised by the existing literature. These questions serve to guide the next stage of the project and to prompt new conversations about how cyber insurance might better incentivise cyber security practices.

INTRODUCTION

In April 2020, reports emerged that Travelex had paid a ransom of $2.3 million to restore its services after a crippling ransomware attack.[1] Initially, the company claimed that its cyber insurance policy, designed to cover business liability from the impact of cyber incidents, would cover a large part of these outgoings. However, the extent to which the policy covered the company's losses from the ransomware attack remains unclear.[2] Travelex has never stated what sort of policy it has or how much of its losses were covered. In August 2020, Travelex went into administration. The administrators said the

1. Doug Olenick, 'Travelex Paid $2.3 Million Ransom, Report', *SC Magazine*, 10 April 2020, <https://www.scmagazine.com/home/security%20-news/ransomware/travelex-paid-2-3-million-ransom-report/>, accessed 9 November 2020.
2. Robin Pagnamenta, 'Daring $6m Cyber-Heist Could be the Least of Travelex's Woes', *The Telegraph*, 9 January 2020.

impact of this cyber incident, coupled with the coronavirus pandemic, had acutely impacted the business.[3] This case study raises two important points relating to cyber security incentives and the role of cyber insurance. First, the extent to which Travelex's policy covered its losses from the ransomware attack was never disclosed publicly – a fact that promotes perceptions of cyber insurance being a secretive market where pay-outs are hard to unlock.[4] Second, there is no information in the public domain regarding the intricacies of Travelex's cyber insurance policy and whether it directly or indirectly encouraged good cyber behaviours or not.

This case could prove to be significant in the context of cyber security and cyber insurance. Remote working, rapid digitalisation and the need for increased connectivity have already made cyber risk an increasingly significant concern for organisations around the globe.[5] The impact of these overarching trends has been exacerbated by the coronavirus pandemic.[6] At the same time, the frequency and intensity of targeted ransomware operations have started to change cyber risk calculations within businesses.[7] Not only are the number of ransomware attacks increasing, but the payments demanded by attackers are also going up.[8] The threat of financial loss from these new types of cyber risk has brought cyber insurance to the forefront of many companies' agendas.[9] For example, more recently, there have been concerns from the US Treasury about cyber insurers paying ransomware demands.[10]

---

3. Kalyeena Makortoff, 'Travelex Falls into Administration, With Loss of 1,300 Jobs', *The Guardian*, 6 August 2020.
4. Pagnamenta, 'Daring $6m Cyber-Heist Could be the Least of Travelex's Woes'.
5. Cybersecurity and Infrastructure Security Agency (CISA), 'Joint CISA and UK Tip on COVID-19 Cyber Threat Exploitation', 5 May 2020, <https://www.cisa.gov/publication/joint-cisa-and-uk-tip-covid-19-cyber-threat-exploitation>, accessed 8 September 2020.
6. Robert Ackerman Jr, 'The COVID-19 Pandemic and Other Issues Are Stressing Corporate Cyber-Risk Management', RSA Conference, 13 August 2020, <https://www.rsaconference.com/industry-topics/blog/the-covid-19-pandemic-and-other-issues-are-stressing-corporate-cyber-risk-managem>, accessed 9 October 2020.
7. Nathaniel Popper, 'Ransomware Attacks Grow; Crippling Cities and Businesses', *New York Times*, 9 February 2020.
8. Sarah Coble, 'Ransomware Payments on the Rise', *Infosecurity Magazine*, 1 April 2020, <https://www.infosecurity-magazine.com/news/rise-in-ransomware-payments/>, accessed 6 November 2020.
9. Joanne Cracknell and Shauna McAuley, 'Cyber Security Risks During a Pandemic', Willis Towers Watson, 22 July 2020, <https://www.willistowerswatson.com/en-GB/Insights/2020/07/cyber-security-risks-during-a-pandemic>, accessed 7 November 2020.
10. 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.

The RUSI Cyber Research team has partnered with the University of Kent as part of a one-year project, 'Incentivising Cybersecurity through Cyber Insurance' (ICCI). It aims to explore why organisations, particularly SMEs, may or may not feel compelled to introduce sufficient cyber risk-management measures to protect against cyber threats. In particular, the project focuses on the potential relationship between cyber insurance and organisations' cyber security practices. The research will analyse the extent to which cyber insurance could encourage better cyber risk-management practices. A key focus of the research is whether it is possible for cyber insurance to adopt lessons from other mature insurance sectors regarding how they incentivise secure behaviours. This research is funded by the National Cyber Security Centre (NCSC), in collaboration with the Research Institute in Sociotechnical Cyber Security (RISCS).

This Emerging Insights paper sets out some key policy gaps relating to cyber security incentives and the role of cyber insurance. Findings derive from an extensive review of existing material – from industry, government and academia – relating to cyber insurance, cyber security and cyber risk management. The paper is divided into four sections: first, it describes the nascent cyber insurance market; second, it assesses the role of cyber insurance in improving security behaviours and the challenges it faces in achieving this goal; third, it highlights other sectors that the cyber insurance market could learn from; and fourth, it poses a series of policy questions that should inform the direction of further research, including the research project's enquiries.

This paper offers preliminary insights based solely on a review of the existing body of literature, rather than the project's ongoing fieldwork. That fieldwork will feed into the wider project, including a policy research paper due for publication in early March 2021. That phase will provide actionable recommendations based on in-depth primary research with practitioners and policymakers from across government, academia and industry, including a large number of cyber security professionals and cyber insurers.

WHAT IS CYBER INSURANCE?

Cyber insurance allows companies to transfer some of the financial risk associated with cyber incidents to an insurer.[11] It is intended to cover business liability, including first-party costs, and is often presented as a critical component of cyber risk-management approaches within organisations. However, insurance companies include extra services for their customers that are intended to improve cyber security approaches within an organisation. Such services are in the interest of the insurance company, as they are intended to improve an insurer's risk profile. They run the gamut from initial evaluations of cyber security vulnerabilities and

11. Lawrence A Gordon, Martin P Loeb and Tashfeen Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', *Communications of the ACM* (Vol. 46, No. 3, March 2003), pp. 81–85.

access to consultancies to improve their overall cyber security posture, to a range of services to support companies in the event of an incident.

Because of this, some governments around the world have sought to explore the role that cyber insurance could play in incentivising better cyber security behaviours. The UK's NCSC, for example, recently released detailed guidance on how companies should go about purchasing cyber insurance.[12] It highlights seven cyber security questions that businesses should consider before buying insurance.[13] However, insufficient conclusive research has been conducted to adequately explore whether or not cyber insurance does produce such positive cyber security outcomes. As it is a relatively new offering for insurance companies, insurers in recent years have spent a great deal of time clarifying what cyber insurance is, what it does and does not cover, and how to best build profitable portfolios. Some of those issues are covered in this section. In addition, there are further questions about the purpose of cyber insurance, how it functions in practice and the unique challenges it faces to become a fully mature insurance sector with high uptake.

It is important to note that cyber insurance can typically be purchased as either a standalone cyber policy or as part of a wider insurance package that manages other risks. A dedicated cyber insurance policy is often more expensive, but also may offer higher pay-out limits should an incident occur.[14] This kind of policy is also more likely to include the cyber risk tools that are intended to improve cyber security within an organisation.[15] Meanwhile, cyber insurance policies that are part of a broader package can be an attractive proposition in terms of simplicity and affordability.[16]

WHY IS UPTAKE SO LOW?

Cyber insurance uptake has increased over the years within large businesses, particularly in the US and the UK. However, market growth has not met

12. National Cyber Security Centre (NCSC), 'Cyber Insurance Guidance', 6 August 2020, <https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance>, accessed 6 November 2020.
13. *Ibid.*
14. 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 6 November 2020.
15. CISA, 'Cybersecurity Insurance', <https://www.cisa.gov/cybersecurity-insurance>, accessed 9 November 2020.
16. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.

expected rates.[17] The lack of uptake is particularly low among SMEs.[18] As of the 2020 UK Cyber Security Breaches Survey, the UK government estimated that approximately 4% of businesses overall have a specific cyber insurance policy, and only 28% have cyber risks covered as part of a wider insurance policy.[19] For 'micro' firms, the percentage dropped to 2% having a specific cyber insurance policy.[20]

One potential explanation for this is the perceived high cost of such insurance policies and the willingness of companies to invest in them.[21] Appropriately pricing cyber insurance products has been a key limiting factor for the market.[22] Part of the challenge in pricing premiums relates to how exactly insurers should calculate cyber risk.[23] As cyber attacks are a relatively new phenomenon, compared to hurricanes or earthquakes, there is a distinct lack of data about the frequency or impact of cyber incidents. In particular, there is limited data about the true financial implications of a cyber incident, particularly given the rate at which the nature and severity of incidents can change.[24] Moreover, the constantly evolving nature of cyber risks makes it difficult to project what coverage may be required in the coming years, or even months.[25] Due to this lack of data, insurers may struggle to accurately price their premiums in a way that appeals to both their appetite for risk and their customers' spending preferences. They may also struggle to articulate the quantitative benefits of insurance to potential customers in a straightforward and transparent manner.[26]

The constantly evolving nature of cyber risks makes it difficult to project what coverage may be required in the coming years, or even months

The difficulty of assessing the quantitative benefits of cyber insurance can be exacerbated by a widespread lack of understanding about what events cyber insurance could cover. Companies are often unsure of just what claims their

17. Accenture, 'The Global Future of Cyber Insurance – and the London Market's Pivotal Role', 2019, <https://www.cityoflondon.gov.uk/assets/Business/cyber-insurance-report.pdf>, accessed 9 November 2020.
18. Hiscox, 'Hiscox Cyber Readiness Report 2019', April 2019, <https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF>, accessed 9 November 2020.
19. *Ibid.*
20. *Ibid.*
21. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.
22. Marsh and Microsoft, 'By the Numbers: Global Cyber Risk Perception Survey 2018', February 2018, <https://www.marsh.com/us/insights/research/global-cyber-risk-perception-survey.html>, accessed 20 June 2020.
23. Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey', September 2019, <https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf>, accessed 9 November 2020.
24. 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.
25. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.
26. Sachin Shetty et al., 'Reducing Informational Disadvantages to Improve Cyber Risk Management', *The Geneva Papers* (Vol. 43, 2018), pp. 224–38.

insurance will include. Reasons to make a claim can range from human error to being collateral damage from hostile state aggression.[27] Some businesses incorrectly think that other insurance classes will cover the losses from a cyber incident.[28] The nascency of the industry makes it difficult to point to prior case studies of an incident and subsequent pay-outs. Industry figures from Britain suggest that cyber insurers do pay out most of the time, with the Association of British Insurers estimating that their members paid out 99% of claims in 2018.[29] This figure is based on 207 cyber claims made and settled in 2018.[30] This is considered to be one of the highest acceptance rates on claims across the insurance industry.[31] It contrasts sharply with reporting in the US, where the Association of Insurance Commissioners found that of 9,107 claims in 2017 only 28.4% resulted in a payment.[32] The lack of concrete evidence either way points to the perception problem that cyber insurers have regarding claims payments. High-profile coverage of incidents in which insurance companies have not paid out continues to contribute to a popular impression that cyber insurance companies do not pay out.[33]

In addition, many companies do not realise how vulnerable they are to cyber risks and therefore conclude that a cyber insurance policy is not cost effective.[34] The intangible nature of a cyber incident makes it difficult for potential customers to weigh up the value of cyber insurance as compared to the benefits of fire or flood insurance.[35] Surveys show that companies often purchase cyber insurance in a reactive way after a significant incident that has either affected them or one of their close competitors.[36] This

27. CISA, 'Cybersecurity Insurance'.
28. Arthur J Gallagher, '"Silent" Cyber Risk Leaving Millions of UK Businesses Underinsured', 5 February 2020, <https://www.ajg.com/uk/news-and-insights/2020/february/silent-cyber-risk/>, accessed 7 November 2020; Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey'.
29. Association of British Insurers, 'Cyber Insurance Payout Rates at 99%, But Uptake Still Far Too Low', 8 August 2019, <https://www.abi.org.uk/news/news-articles/2019/08/cyber-insurance-payout-rates-at-99-but-uptake-still-far-too-low/>, accessed 6 November 2020.
30. *Ibid.*
31. *Ibid.*
32. CISA, 'Assessment of the Cyber Insurance Market', July 2019, p. 5.
33. Sarah Stephens, 'How Cyber Insurance Can Still Leave You Vulnerable to Risks', *Computer Fraud and Security* (Vol. 2020, No. 2, February 2020), pp. 2–4; Phil Muncaster, 'Zurich Refuses to Pay Out for NotPetya "Act of War"', *Infosecurity Magazine*, 11 January 2019, <https://www.infosecurity-magazine.com/news/zurich-refuses-to-pay-out-for/>, accessed 6 November 2020; Lisa Vaas, 'We Don't Cover Stupid, Says Cyber Insurer That's Fighting a Payout', *Naked Security*, 28 May 2015, <https://nakedsecurity.sophos.com/2015/05/28/we-dont-cover-stupid-says-cyber-insurer-thats-fighting-a-payout/>, accessed 6 November 2020.
34. Department of Digital, Culture, Media and Sport (DCMS), 'Cyber Security Breaches Survey 2019', 2 July 2019, p. 25.
35. Stephens, 'How Cyber Insurance Can Still Leave You Vulnerable to Risks'.
36. Bernard, 'Overcoming Challenges to Cyber Insurance Growth'.

suggests that a lack of cyber awareness is a big factor in the lack of uptake.[37] However, the General Data Protection Regulation (GDPR) and its resulting fines are also thought to have helped to make the risks of cyber breaches more tangible.[38]

From the difficulty of calculating premiums, uncertainty around coverage, concerns insurers will not pay out after an incident and a low perception of risk among businesses, it is easy to understand why cyber insurance uptake has been much lower than was expected by the cyber community.[39] Although companies repeatedly state that cyber risks and incidents rank among their top concerns, the cyber insurance industry still needs to build trust in its products and better demonstrate the benefits (some of which relate to security). These are some of the reasons why cyber insurance uptake has been so low to date.[40]

CAN CYBER INSURANCE IMPROVE SECURITY PRACTICES?

Cyber insurers have a financial interest in reducing the number of cyber incidents to avoid claims, as well as mitigating the impact of events in order to limit the amount they must pay out to clients. While most organisations see cyber incidents as a low-probability, high-impact event, research revealed that cyber insurers address such incidents regularly as part of their business model.[41] Some invest in full-time cyber security professionals to advise clients on the best ways to mitigate their exposure to cyber risks.[42] For SMEs, these services often prove too expensive to recruit in-house. Cyber insurers therefore can help to identify particular experts to mitigate risk.[43] Insurers can quickly assemble teams with relevant expertise to support their clients before, during and after an incident.[44] This includes forensics teams and breach counsel,[45] and public relations and other cyber crisis responders.[46] Companies can often gain access – for example, free access or direction to key services – to these resources through their cyber

37. *Ibid.*
38. Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey', p. 24.
39. *Ibid.*, pp. 22–30.
40. *Ibid.*; CISA, 'Cybersecurity Insurance'.
41. HM Government, 'UK Cyber Security: The Role of Insurance in Managing and Mitigating the Risk', March 2015, p. 3.
42. *Ibid.*
43. Daniel W Woods and Tyler Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', *Security and Privacy* (Vol. 18, No. 1, 2020), pp. 21–27; Marsh and Microsoft, '2019 Global Cyber Risk Perception Survey'.
44. HM Government, 'UK Cyber Security', p. 17.
45. DCMS, 'Cyber Security Breaches Survey 2020', 26 March 2020, p. 25.
46. Richard Knight and Jason R C Nurse, 'A Framework for Effective Corporate Communication After Cyber Security Incidents', *Computers and Security* (Vol. 99, December 2020).

insurance policy.[47] A pertinent, and somewhat unclear, question that arises here is the extent to which organisations remain covered if they fail to adopt the practices suggested by insurers.

Some experts argue that cyber insurance encourages companies to assess their exposure to cyber risk.[48] For example, cyber insurers can help to raise awareness around risk management by introducing clear benchmarks for companies seeking to improve their cyber security.[49] Insurance companies can also increase companies' understanding of their exposure and support them by continuously assessing the risks they face.[50] The expertise and awareness that cyber insurance companies offer can increase knowledge about appropriate risk mitigation measures.

This expertise includes consolidated information and data. Cyber insurers collect a significant pool of data about the types of cyber risk companies face. In doing so, they would be well equipped to put together comprehensive models that explain, and even quantify, elements of cyber risk.[51] These models can help to determine what measures might be most effective, although the dynamic nature of the field and the shifting threat landscape make collecting up-to-date data an enduring challenge.[52] There have already been initiatives by insurers – such as Cyber Catalyst by Marsh[53] – to define cyber products that are perceived as effective at reducing cyber risk.

Insurance can also make the risks from poor cyber security more quantifiable. Insurance requirements help to ensure that initial measures are not a one-time expenditure, but rather are reviewed and renewed as necessary to comply with contractual obligations.[54] Companies can be incentivised to introduce cyber controls to avoid the potential financial loss as a consequence of neglecting certain safety measures that are required by insurers.[55] The topic of ransomware and payments to cyber-criminals is also pertinent to discussions on cyber insurance, given the ongoing deliberations regarding whether ransomware payments facilitated by cyber insurers are

47. Sauhin A Talesh, 'Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business', *Law and Social Inquiry* (Vol. 43, No. 2, Spring 2018), p. 417.
48. OECD, 'Enhancing the Role of Insurance in Cyber Risk Management', December 2017, p. 7.
49. *Ibid.*
50. Accenture, 'The Global Future of Cyber Insurance – and the London Market's Pivotal Role', p. 12.
51. Gordon, Loeb and Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', p. 82.
52. Nurse et al., 'The Data That Drives Cyber Insurance'.
53. Marsh, 'Cyber Catalyst 2020 Risk Outlook', March 2020.
54. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 22.
55. Gordon, Loeb and Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', p. 82.

leading to an increasing number of ransomware attacks.[56] Such notions have also fuelled wider concerns from parties including the US Treasury.[57]

This paper showcases existing literature that looks at how cyber insurance could significantly increase cyber security and resilience. One development in the field is the belief that insurance is fundamental to cyber risk management.[58] This model advocates a balance between security controls and insurance to allow cyber risk to be reduced to acceptable levels for both the organisation and the insurer. However, there are still sceptics who believe that the role of cyber insurance in cyber risk management has been overplayed and will remain limited.[59]

One area that requires further examination is the varying approaches that cyber insurers may take to assess cyber risk within organisations. While some may take a high-level strategic approach to risk management (such as audits or questionnaires), including the use of a variety of cyber risk-management frameworks,[60] other cyber insurers may take a more technical deep dive into the risk held within an organisation. An in-depth understanding of this nuance is missing in the literature. The different services cyber insurers provide to assess cyber risk matters. They will clearly have an impact on the types of secure behaviours adopted by organisations.

CYBER INSURANCE SCEPTICISM

Case studies of positive cyber insurance outcomes are limited. The existing evidence base is largely theoretical and assumes that taking out a policy will result in improved cyber security behaviours. Sceptics can point to low cyber insurance uptake, ambiguity around defining 'good' security behaviours, the incentives for insurers to lower prices and requirements, and the potential for cyber insurance to promote poor security behaviours.

56. Marsh, 'Cyber Insurance Is Supporting the Fight Against Ransomware', October 2019, <https://www.marsh.com/us/insights/research/cyber-insurance-supporting-fight-against-ransomware.html>, accessed 9 November 2020.
57. Simpson, 'U.S. Treasury Warns Cyber Insurers Against Paying Ransom Demands'.
58. Gordon, Loeb and Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', pp. 81–85.
59. Walter S Baer and Andrew Parkinson, 'Cyberinsurance in IT Security Management', *Security and Privacy* (Vol. 5, No. 3, May/June 2007), pp. 50–56; Inger Anne Tøndel et al., 'Using Cyber-Insurance as a Risk Management Strategy: Knowledge Gaps and Recommendations for Further Research', SINTEF, 11 November 2015, <https://core.ac.uk/download/pdf/52131083.pdf>, accessed 18 June 2020.
60. Daniel Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms', *Journal of Internet Services and Applications* (Vol. 8, 2017).

As mentioned, cyber insurance uptake has been much lower than predicted. This is a particular concern for SMEs.[61] The cost of a policy can be a deterrent for businesses. Although insurers offer discounts if a company demonstrates good cyber security behaviours, they are often dwarfed by the price of the overall premium.[62] Organisations may see the price of a policy and (often incorrectly) assess that their cyber risk is not high enough to justify the outlay.

There is also ambiguity over what constitutes 'good' cyber security behaviours. Cyber security standards[63] play a role in how policies are underwritten and what controls organisations introduce to improve their cyber security.[64] Yet, different cyber insurers require different security controls to underwrite a policy.[65] There is a range of formal frameworks, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the UK's Cyber Essentials.[66] While there are commonalities across standards, controls also vary, especially with regard to the metrics used to measure success.[67] Cyber Essentials is a well-known UK government-backed scheme, but some argue that it is merely a 'box-ticking' exercise in cyber security which could lead to sub-optimal cyber security outcomes.[68]

Another concern relates to market incentives and to what extent cyber insurers adequately analyse customers' cyber security posture prior to offering coverage.[69] As the cyber insurance market continues to grow, insurers face increasing competition for customers and such dynamics could cause companies to lower the price of their products. Lower prices could lead to a decrease in requirements (namely, evidence of security controls) and a lower threshold to obtain a policy.[70] In this scenario, there is less incentive

61. Hiscox, 'Hiscox Cyber Readiness Report 2019', p. 2.
62. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 23.
63. See, for example, NIST, 'Cybersecurity Framework', <https://www.nist.gov/cyberframework>, accessed 10 November 2020; 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.
64. See, for example, Marsh, 'Cyber Catalyst 2020 Risk Outlook'.
65. Woods et al., 'Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms', p. 1.
66. NIST, 'Cybersecurity Framework'; NCSC, 'Cyber Essentials'.
67. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 23.
68. Christopher Decker, 'Goals-Based and Rules-Based Approaches to Regulation', Department for Business, Energy and Industrial Strategy (BEIS), BEIS Research Paper No. 8, May 2018.
69. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 23.
70. Nurse et al., 'The Data That Drives Cyber Insurance'.

for insurers to encourage better cyber security behaviours,[71] while insurers who do not lower their prices may be uncertain of making a profit.[72] This phenomenon is colloquially referred to as a 'race to the bottom'.

Some argue that taking out a cyber insurance policy could actually discourage secure behaviours, a concept known as 'moral hazard'.[73] Several studies have found 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 anyway.[74] The moral hazard phenomenon, which argues that protected groups could take on more risk, is true for the insurance sector as a whole.[75] It has the potential to drive up insurance premiums, placing an increased financial burden on companies who invest in preventive measures, as well as insurance.[76] Another complexity is the uncertainty around security controls more broadly, and the reality that little is ultimately known about what the most effective security controls at mitigating cyber risk are today.[77] Therefore, insurers may themselves be unclear about what controls to require to prevent moral hazard concerns.

Another area of contention relates to what extent governments should intervene in the cyber insurance industry to increase national cyber resilience. One drastic intervention would make cyber insurance mandatory, putting it on the same statutory footing as car and employee liability insurance. Other interventions could include mandating specified security standards or standardising language in cyber insurance policies to simplify understanding. The UK government has already explored some soft interventions. For example, the NCSC recently released a guide to purchasing

71. Nikhil Shetty et al., 'Competitive Cyber-Insurance and Internet Security', in Tyler Moore, David Pym and Christos Ioannidis (eds), *Economics of Information Security and Privacy* (Berlin: Springer, 2010), pp. 229–47.
72. Ranjan Pal et al., 'Will Cyber-Insurance Improve Network Security? A Market Analysis', in IEEE INFOCOM 2014 – IEEE Conference on Computer Communications, Toronto, 27 April–2 May 2014, <http://bourbon.usc.edu/leana/papers/PalGPH14.pdf>, accessed 10 November 2020.
73. Liam M D Bailey, 'Mitigating Moral Hazard in Cyber-Risk Insurance', *Journal of Law and Cyber Warfare* (Vol. 3, No. 1, Spring 2014), pp. 1–42.
74. 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.
75. James Hedlund, 'Risky Business: Safety Regulations, Risk Compensation, and Individual Behavior', *Injury Prevention* (Vol. 6, No. 2, June 2000), pp. 82–90.
76. Woods and Moore, 'Does Insurance Have a Future in Governing Cyber Security?', p. 26.
77. 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, 30 November 2016, <https://www.cs.ox.ac.uk/files/8869/The_Relative_Effectiveness_of_widely_used_Risk_Controls_and_the_Real_Val....pdf>, accessed 9 November 2020.

cyber insurance.[78] In the US, the topic of cyber insurance has been widely covered from a government perspective, with purchase advice available from the Federal Trade Commission (FTC)[79] and ongoing discussions by the Cybersecurity and Infrastructure Security Agency (CISA).[80] The EU has also explored the utility of cyber insurance through reports into good practices[81] and recommendations to address challenges facing the industry.[82]

Finally, there are still doubts about how exactly the insurance industry should try to incentivise better security behaviours. Suggestions often include lowering premiums or deductibles for companies who comply with minimum security standards (such as achieving certification from Cyber Essentials, NIST CSF or a similar scheme). By linking a policy to an independent assessment, cyber insurance companies can then adjust premiums depending on the findings.[83] Client organisations that do not have good cyber hygiene, or secure systems, would therefore face higher premiums.[84] Meanwhile, in the event of a cyber incident, deductibles would be attached to the initial fixed price tags.[85] Some argue that insurance companies have managed their risks with broad exclusion language that exempts them from paying out.[86] One way to overcome these ambiguities could be for governments to recommend a minimum set of controls for an organisation to be eligible for cyber insurance.[87]

78. NCSC, 'Cyber Insurance Guidance'.
79. Federal Trade Commission, 'Protecting Small Businesses', <https://www.ftc.gov/tips-advice/business-center/small-businesses>, accessed 30 November 2020.
80. CISA, 'Cybersecurity Insurance'.
81. European Union Agency for Network and Information Security (ENISA), *Cyber Insurance: Recent Advances, Good Practices and Challenges* (Heraklion: ENISA, 2016).
82. ENISA, *Commonality of Risk Assessment Language in Cyber Insurance: Recommendations on Cyber Insurance* (Heraklion: ENISA, 2017).
83. Fabio Martinelli et al., 'Preventing the Drop in Security Investments for Non-Competitive Cyber-Insurance Market', in Nora Cuppens et al. (eds), *Risks and Security of Internet and Systems* (Dinard: CRiSIS, 2017), pp. 159–74; Nour Aburish, Annie Fixler and Michael Hsieh, 'The Role of Cyber Insurance in Securing the Private Sector', Foundation for Defense of Democracies, 13 September 2019, <https://www.fdd.org/analysis/2019/09/11/cyber-insurance/>, accessed 10 September 2020.
84. Woods and Moore, 'Does Insurance Have a Future in Governing Cybersecurity?', p. 22.
85. Gordon, Loeb and Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', p. 83.
86. *Forbes*, 'Cyber Insurance: A Study in Fine Print', 14 August 2019, <https://www.forbes.com/sites/insights-ibmresiliency/2019/08/14/cyber-insurance-a-study-in-fine-print/?sh=492015ae2d58>, accessed 30 November 2020.
87. Cabinet Office, 'Minimum Cyber Security Standard', 25 June 2018, <https://www.gov.uk/government/publications/the-minimum-cyber-security-standard>, accessed 30 November 2020.

HOW CAN CYBER INSURANCE LEARN FROM OTHER INSURANCE SECTORS?

Many of the problems facing cyber insurance are not unprecedented. Other sectors such as property, car, terrorism, health and maritime have had similar strategic challenges. Existing research into the challenges faced by other sectors could help the cyber insurance sector to draw on these experiences.

Analysts often draw parallels between property, car and cyber insurance, owing to the comparable security requirements. For example, it would be difficult to purchase home insurance without providing evidence of a suitable lock on your front door. Similarly, it is not possible to purchase car insurance without a driving licence and almost impossible if a car does not have seatbelts.[88] In addition, homeowners can qualify for reduced premiums by installing burglar alarms or introducing barriers, such as a high fence. Incentives are important too. Motorists are incentivised to drive safely partly due to the threat of increased premiums should they end up in an incident. Meanwhile, telematics (digital vehicle monitoring) enable insurers to monitor driver behaviour by sending both data and communications back and forth between a vehicle and a central management system.[89] This way, insurance companies can adjust premiums in a proactive manner based on individual driver analytics.

Terrorism insurance shares some similarities with cyber insurance. As both are man-made or anthropogenic risks, they share a level of unpredictability that natural disasters or fire do not have. As such, gathering consistent data is a challenge for both. This has led to uncertainty about the true scale of the risk that is being underwritten. Terrorism insurance was designed to meet unique needs and there was a significant shortage of industry expertise, as well as data to construct premiums, in the early days of the industry.[90] Some say that the purchase of terrorism insurance has often been driven by large incidents, similar to the way that large breaches drive uptake in cyber insurance.[91] To add to the complexity, companies that purchase terrorism insurance also have a significant potential for an adverse selection problem similar to that for cyber insurance, in that companies that see the value in terrorism insurance may be disproportionately likely to suffer from terrorist attacks.[92]

88. David Bjerklie, 'The Hidden Dangers of Seat Belts', *Time*, 30 November 2006.
89. Mark Stevenson et al., 'The Effects of Feedback and Incentive-Based Insurance on Driving Behaviours: Study Approach and Protocols', *Injury Prevention* (Vol. 24, No. 1, 2018), pp. 89–93.
90. Insurance Information Institute, 'Background On: Terrorism Risk and Insurance', 16 December 2019, <https://www.iii.org/article/background-on-terrorism-risk-and-insurance>, accessed 9 November 2020.
91. DCMS, 'Cyber Security Breaches Survey 2020'.
92. Gordon, Loeb and Sohail, 'A Framework for Using Insurance for Cyber-Risk Management', p. 82.

Following on from terrorist incidents in the 1990s and the significant impact of 9/11, the terrorism insurance industry realised that it had not fully accounted for the risk it was underwriting. This risk was recognised by governments who issued guarantees or provided financial backing for this type of insurance. In the UK, starting in the 1990s, the government issued a guarantee to Pool Re – a terrorism insurance company – that would cover any costs relating to a terrorist incident above a certain threshold.[93] Similarly in the US, the government has created the Terrorism Risk Insurance Act to provide federal reinsurance to any property and casualty insurer who offers terrorism insurance.[94] In doing so, it has agreed to reimburse insurers for a portion of losses of up to $100 billion on commercial policies.[95] Governments could have a similar role in cyber insurance, owing to the potential fallout from a catastrophic cyber incident.

Moral hazard is a significant challenge for the health insurance sector. Some individuals may neglect preventive care once they take out a policy,[96] thinking that their insurance policy will cover the cost of treating an illness.[97] This creates financial problems for insurers, as preventive care is often less expensive than the cost of treating a serious condition later on.[98] It also has a detrimental effect for the purchaser, who could undergo a lengthy hospital stay or worse.[99] A parallel problem in cyber security is when companies do not spend money on cyber defence because they assume that the insurance company will compensate them in the event of an incident.[100] The health insurance industry has spent a great deal of time looking into the problem of moral hazard. Through an investigation into the methods that they use, insurers could be informed about how to better incentivise cyber-related preventive measures among purchasers of cyber insurance.

There are doubts about how exactly the insurance industry should try to incentivise better security behaviours

Encouraging healthy individuals to purchase health insurance is also an enduring challenge. The rollout of the US's Affordable Care Act revealed that many young and healthy individuals often failed to purchase health insurance.[101] Some young individuals, without pre-existing conditions, felt

93. Daniel M Hoffman, 'Advancing Accumulation Risk Management in Cyber Insurance: Prerequisites for the Development of a Sustainable Cyber Risk Insurance Market', The Geneva Association, August 2018, p. 20.
94. Congressional Budget Office, 'Federal Reinsurance for Terrorism Risk: An Update', January 2015, p. 1.
95. *Ibid.*
96. Hui, Hui and Yue, 'Cyber Insurance and Risk Management', p. 3.
97. *Ibid.*
98. R L Kane et al., 'Economic Incentives for Preventive Care: Summary', Agency for Healthcare Research and Quality, August 2004, <https://www.ncbi.nlm.nih.gov/books/NBK11845/>, accessed 9 November 2020.
99. *Ibid.*
100. Hui, Hui and Yue, 'Cyber Insurance and Risk Management', p. 3.
101. Samyukta Mullangi, A Mark Fendrick and Kavita Patel, 'How to Persuade the Young and the Healthy to Sign Up for Health Insurance', *Harvard Business Review*, 18 January 2018.

that they were not exposed to the risks that health insurance is intended to offset. Balanced against the expense of a premium, these individuals concluded that the cost savings are of greater benefit than the low health risk. However, this lack of uptake raises premiums elsewhere. In this scenario, only high-risk individuals, with the potential for expensive medical expenses, purchase health insurance. Consequently, insurers are unable to offset pay-outs for high-risk cases against the premiums of low-risk individuals.[102] Cyber insurance has similar gaps with uptake where many companies do not feel that the risk is high enough to warrant the purchase of insurance. Also, there is an argument that the more a company spends on its own risk-mitigation practices, the less motivation they have to subsidise the poor risk-management practices of others. To increase uptake, the health insurance sector focuses on education and awareness campaigns and adjusts premiums and deductibles to better suit the needs of a low-risk customer.[103] Such campaigns may be applicable to the cyber insurance industry as well.

Maritime insurance is one of the oldest classes of insurance on the market. Historically, insurers have worked with the maritime industry to mitigate and manage the risk. It is an iterative process depending on the context at the time. For example, insurers may study ship construction and pirate attack patterns.[104] In the early 1900s, insurance companies intervened to study the risks caused by boiler explosions.[105] More recently, maritime insurance has had to contend with the risks posed by increases in piracy.[106] As the maritime insurance industry has such a long and well-explored history, there may be processes or lessons that can be applied to emerging insurance sectors, such as cyber insurance.

Kidnap and ransom (K&R) insurance also forms another pertinent class of insurance that shares some similarities with cyber. This is driven especially by the recent proliferation of ransomware attacks over the past 24 months targeting a range of organisations from hospitals to businesses,[107] and even some insurers.[108] K&R policies have been seen to cover

102. *Ibid.*
103. *Ibid.*
104. Ariel E Levite, Scott Kannry and Wyatt Hoffman, 'Addressing the Private Sector Cybersecurity Predicament: The Indispensable Role of Insurance', Carnegie Endowment for International Peace, October 2018, p. 11.
105. *Ibid.*
106. Costas Lambrou, 'The Implications of Piracy on Marine Insurance: Some Considerations for the Shipowner', *WMU Journal of Maritime Affairs* (Vol. 11, 2012), pp. 129–41.
107. Dustin Volz and Robert McMillan, 'Hackers Hit Hospitals in Disruptive Ransomware Attack', *Wall Street Journal*, 29 October 2020.
108. Sergiu Gatlan, 'Ransomware Hits US-Based J. Gallagher Insurance Giant', Bleeping Computer, 29 September 2020, <https://www.bleepingcomputer.com/news/security/ransomware-hits-us-based-arthur-j-gallagher-insurance-giant/>, accessed 30 November 2020.

ransoms, response consultancy services, fees for negotiators and more.[109] These are the same activities now central in cases of ransomware attacks; therefore, there are undoubtedly many lessons that can be learnt from this insurance domain.

The direct connection between the incentives used by other insurance sectors to increase uptake and cyber insurance requires further enquiry. This section has merely listed some of the approaches taken by other sectors. For this ongoing research project, primary research into the approaches of other insurance sectors could identify what exact interventions the cyber insurance market could successfully mirror.

IMPLICATIONS AND FURTHER QUESTIONS

Based on this paper, ICCI project members will perform primary research into the ways in which cyber insurance may be helpful in incentivising companies to improve their cyber security systems and risk-management practices. Full recommendations will be presented in a research paper due for publication in March 2021, which will propose specific and actionable policy recommendations. In doing so, the project seeks to inform and complement the existing work being conducted by the UK government on how cyber security incentives and regulation can overcome existing barriers to improving cyber security practices.[110] Project members expect that there are also wider applications of this research beyond the UK, and that findings will also be able to complement and provide additional insights to governments and practitioners in the US, EU and Asia.

The following policy questions have emerged from the preliminary stages of this research project, based on an extensive literature review. They set the stage for the project's continuing investigation into cyber security incentives and the role of cyber insurance:

- What is the role of the cyber insurance market in the context of cyber risk management for large, medium and small organisations?

109. Gallagher, 'Kidnap and Ransom Insurance', <https://www.ajg.com/uk/corporate-insurance/crisis-management/kidnap-and-ransom-insurance/>, accessed 30 November 2020; AIG, 'Crisis Solution', <https://www.aig.co.uk/business-insurance/innovative-products/business-insurance-products/financial-lines/kidnap-ransom-extortion>, accessed 30 November 2020; Beazley, 'Kidnap and Ransom', <https://www.beazley.com/london_market/political_risks_and_contingency/kidnap_and_ransom.html>, accessed 30 November 2020.
110. These barriers are: the lack of ability to manage cyber risks, the complexity of digital environments and the lack of commercial rationale to invest in cyber security practices. See DCMS, 'Cyber Security Incentives & Regulation Review: Summary of Responses to the Call for Evidence', 27 August 2020.

- To what extent can cyber insurance companies act to incentivise better cyber security practices and systems within businesses? What, if any, are the conditions required for this to occur?
- To what extent can cyber insurance negatively influence cyber security practices or systems in businesses (for example, how real is the issue of moral hazard or concerns such as the 'race to the bottom')?
- If cyber insurance can have a positive impact on businesses, how can the positive influences be best championed?
- What is the role of government in maximising any positive impacts of cyber security from cyber insurance? How could it alleviate any concerns?
- Are there other insurance classes that may provide lessons for the cyber insurance ecosystem, particularly as it relates to influencing better risk-management behaviours?
- Are there differences in the way cyber insurers approach assessing risk and underwriting policies? If so, do different approaches have different impacts on cyber security practices?

Through an exploration of these questions, the ICCI project aims to provide valuable insight for policymakers currently seeking ways to optimise the potential impact of cyber insurance on cyber security. Improving cyber security across society will generate positive outcomes, not only for the organisations, but for whole-of-society resilience.

ABOUT THE AUTHORS

James Sullivan is Head of Cyber Research at RUSI. He leads a research team that takes what can be a complex and technical subject and communicates information in plain language for non-technical audiences. RUSI Cyber Research focuses on five thematic areas: the cyber threat landscape; improving defence and resilience; the role of legislation and regulation; online education, awareness and behaviour; and the cyber ecosystem. James joined RUSI from Deloitte's Cyber Risk team, where he provided analysis on the cyber threat landscape and advised clients on cyber risk-management strategies. Prior to this, James worked at the National Crime Agency as an Intelligence Analyst specialising in cybercrime threats. His research interests include cyber security, the spread of terrorism and violent extremism in cyberspace, online disinformation campaigns, and the role of emerging technology in defence and security. He holds an MSc in Security Studies from University College London.

Jason R C Nurse is an Associate Professor in Cyber Security at the University of Kent. He is also a Visiting Academic at the University of Oxford, and a Visiting Fellow in Defence and Security at Cranfield University. His research concentrates on investigating interdisciplinary approaches to enhance and maintain cyber security for organisations and governments. This considers topics such as cyber insurance, privacy and security in the Internet of Things, cyber resilience, and human factors of cyber crime. Jason holds a PhD from

the University of Warwick in cyber security for organisations, an MSc from the University of Hull and a BSc from the University of the West Indies.

The authors would like to thank Rebecca Lucas for her vital contribution to this paper and the project as a whole. This includes conducting the wider literature review and other research activities during the first half of this project. The authors would also like to thank RUSI Cyber Research Analyst Jamie MacColl who helped to finalise the paper during the peer review process.

About RUSI

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 189 years.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies. RUSI is a registered charity (No. 210639).

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)