Computers & Security 128 (2023) 103162

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Between a rock and a hard(ening) place: Cyber insurance in the ransomware era

Gareth Mott[a], Sarah Turner[b], Jason R.C. Nurse[b,*], Jamie MacColl[c], James Sullivan[c], Anna Cartwright[d], Edward Cartwright[e]

[a] School of Politics and International Relations and Institute of Cyber Security for Society (iCSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom
[b] School of Computing and Institute of Cyber Security for Society (iCSS), University of Kent, Canterbury, Kent CT2 7NF, United Kingdom
[c] Royal United Services Institute (RUSI), 61 Whitehall, London, SW1A 2ET, United Kingdom
[d] Oxford Brookes Business School, Oxford Brookes University, Oxford, OX3 0BP, United Kingdom
[e] Department of Accounting, Finance and Economics, De Montfort University, Leicester, LE1 9BH, United Kingdom

ARTICLE INFO

Article history:
Received 20 November 2022
Revised 20 February 2023
Accepted 24 February 2023
Available online 27 February 2023

Keywords:
Cyber security
Ransomware
Cyber insurance
Security incidents
Harms
Cyber policy
Resilience
Critical national infrastructure
Malware

ABSTRACT

Cyber insurance and ransomware are two of the most studied areas within security research and practice to date, and their interplay continues to raise concerns in industry and government. This article offers substantial new insights and analysis into the complex question of whether cyber insurance can help organisations in mitigating the threat of ransomware, particularly its impacts. Having conducted an interview or workshop with 96 industry professionals spanning the cyber insurance, cyber security, ransomware negotiations, policy, and law enforcement sectors, we identify that ransomware has been a key cause of the 'hardening' of the cyber insurance market, which is exhibited at almost all levels of the market. Such hardening has been beneficial in raising the security standards required prior to purchase, but has also created a situation where some organisations may not be able to acquire viable cyber insurance at all. In presenting the outcomes of our thematic analysis of the interview and workshop outputs, the paper provides significant new empirical evidence to support the theory that cyber insurance can act as a form of governance for improving cyber security amongst organisations. Nonetheless, the hardening market does nothing to increase the penetration of cyber insurance. Questions were also raised as to the likelihood of unintended unethical – and potentially illegal – outcomes given the professionalisation of a remediation process that has to determine the most cost-effective solution to an organisation being held ransom. We conclude that insurance, at best, can help to mitigate the ransomware threat for those that can access it, as part of a wider basket of actions that must also come from different stakeholders.

1. Introduction

Ransomware is a form of malware that disrupts access to a computer system or exfiltrates valuable data. The operator of the infected machine is instructed to pay a ransom to decrypt their files and/or for exfiltrated data to be deleted. Perpetrators of ransomware attacks have used a variety of attack vectors to initially compromise target machines with some of the most prominent attack vectors in the last two years being phishing, exposed RDP ports, vulnerable remote access services, and corrupted webpages (National Cyber Security Centre, 2018; Coveware, 2020, 2021; Reshmi, 2021). Ransomware has now come to be regarded as one of the most common forms of malware, particularly from 2018 onwards (Agrafiotis et al., 2018; Lallie et al., 2020). In a February 2022 joint Cybersecurity Advisory with the FBI, NSA, Australian ACSC and British NCSC, the USA's Cybersecurity and Infrastructure Security Agency warned that ransomware had become one of the most disruptive global cyber threats, with potentially devastating consequences; with particular concerns surrounding vulnerabilities in critical infrastructure (CISA, 2022). Additionally, in October and November 2022, the Biden administration convened an International Counter-Ransomware Initiative (CRI) Summit, drawing together leaders from 36 countries and the EU (Brumfield, 2022). In a consolidation of coordinated effort(s), the CRI announced that it would implement a range of measures, including the formation of

* Corresponding author.
E-mail address: J.R.C.Nurse@kent.ac.uk (J.R.C. Nurse).

https://doi.org/10.1016/j.cose.2023.103162

an Australian-led counter-ransomware taskforce, improve information sharing, undertake bi-annual counter-ransomware exercises, and the production of a ransomware-specific 'investigator's toolkit' for stakeholders (White House, 2022).

Increased awareness of the potential risks posed by ransomware has prompted general improvements in the cyber security of organisations; particularly in terms of up-to-date and segmented backups (Connolly and Wall, 2019; Databarracks, 2021). If a victim organisation has a functional and relatively fast surviving backup, in principle, this significantly reduces incentives to pay a ransom demand; uninfected versions of vital systems and files can be restored. Recognising this, from 2019 onwards, ransomware gangs have sought to apply an additional form of leverage against their victims, as part of a 'double extortion' approach (Kenneally et al., 2020; Logan et al., 2021). Accordingly, before deploying the malicious encryption, the criminals may exfiltrate data and use the threat of public data leakage, sale of data to competitors, or cold-calling clients, to apply further pressure on the victim organisation. Seen in this light, ransomware harshly marries two severe risks for organisations: prolonged business interruption and extensive data privacy breach.

Resilience against cyberattacks including ransomware may be improved through a combination of mechanisms. The acquisition of a cyber insurance policy is one measure that organisations may undertake to increase their capacity to withstand a ransomware incident, amongst other cyber risks. The core raison d'être of cyber insurance is to offset the financial risk posed by cyber incidents, thereby increasing the insured's resilience; this would include for instance, recovery, incident investigations, and business interruption costs. Bespoke cyber insurance policies – as opposed to broader insurance policies that include an add-on for cyber risk cover – often go further than a transactional offsetting of risk: these products may also include guidance on effective cyber security practices, free or discounted technical solutions, as well as post-breach remediation (Bailey, 2014; Franke, 2017; Woods and Moore, 2020; MacColl et al., 2021). Cyber insurance products have been recognised as a potential growth area for the insurance market, with some estimates indicating that a market value of $20.56 billion could be reached in 2025 (Rafferty, 2021), which would represent a more than tenfold increase on the 2015 market size.

Whilst insurance may be viewed as an appropriate technique for companies to partially address the threat of ransomware, there have been numerous conflicting perspectives on its influence. For instance, some argue that insurance – via its payments of ransoms – is exacerbating the ransomware crisis (Dudley, 2019; Jenkins and Ventham, 2022). There have even been reports of organisations targeted by ransomware gangs because they have insurance (Cluley, 2021). Conversely, others posit that cyber insurance is part of the solution against such attacks by providing access to third party services and, if necessary, paying the ransom to allow the organisation – be it a hospital, school, or national oil pipeline systems – to resume its services (Jenkins and Ventham, 2022).

This article seeks to advance these discussions by investigating the question: is cyber insurance helping to mitigate the threat of ransomware, particularly its impacts? We are especially interested in impacts due to the traditional position of insurance as a reactive and resilience mechanism, and scope our work primarily to the UK given its maturity (though there are undoubtedly findings that have wider relevance). The analysis and findings presented are drawn from interviews with 65 industry professionals and a follow-up workshop with 49 (31 new) industry stakeholders, all of whom have experience of working in the UK in their respective fields. Together, these studies engaged with a significant cross-section of representatives from the cyber insurance ecosystem including underwriters, claims handlers, reinsurers, brokers, recruiters, insurance buyers, industry associations and regulators, and government employees. To date, this is one of the largest in-depth qualitative studies on the cyber insurance industry and its interaction with the topic of security threats such as ransomware.

We identify a range of pertinent findings at a critical juncture in the ongoing maturation of the UK market. The article finds that cyber insurance has generally become less accessible amidst a hardening of the market, although this may not have yet impacted the market targeted at the smallest insureds. Additionally, some prospective insureds may be unable to acquire a cyber insurance policy – irrespective of their cyber security practices – by virtue of their industry. Amidst this market hardening, potential demand is increasing, because ransomware has articulated cyber security in crystallising financial costs, particularly in terms of business interruption and data breaches (Li and Mamon, 2023). However, the degree of the hardening market may force some prospective insureds to query the prospect value of cyber insurance; instead seeking alternative solutions such as self-insurance.

There is, nonetheless, scope for cyber insurance to reduce the threat of ransomware, particularly with respect to the provision of pre- and post-breach services that seek to reduce the likelihood of a ransomware attack occurring and increase the resilience of an organisation in the event of an incident. Furthermore, the hardening of the market and the raising of minimum cyber security standards may be forcing prospective insureds to hasten or deepen good cyber security practices; particularly with respect to secure backup solutions and multi-factor authentication (MFA) solutions. At the same time, however, this is an evolving phenomenon, with insurers seeking to improve their insight into prospective insureds, to use claims data to inform underwriting, and potentially to enforce good behaviour through warranties. One potential downside to mandated security controls and the improved insights into prospective insureds is the increased inaccessibility of cyber insurance products; without a clear alternative to cyber insurance, some organisations may not be able to transfer their risk and may thus be acutely impacted by potential ransomware incidents.

The ensuing article is structured in five sections. Firstly, the article presents the state-of-the-art literature and arguments relating to the interrelationship between cyber insurance and ransomware. Of particular focus is the challenge presented by the reality that cyber insurance is a relatively novel product, and ransomware is a dynamic risk. Secondly, the article outlines the qualitative methodological approach underpinning the research. Thirdly, the results of this qualitative research are outlined, establishing the basis for the fourth section; a discussion. Finally, a conclusion summarises the main contributions of the research, and outlines scope for further work.

2. Ransomware and cyber insurance: The state of the field

2.1. Two compounding problems: novel product and novel risk

Endeavours to assess the equilibrium between accurate or realistic pricing of cyber insurance premiums (Uuganbayar et al., 2021), mapping the costs of ransomware across differing insureds, as well as identifying the most-effective cyber security practices, are complicated by two compounding problems globally. Firstly, cyber insurance is a relatively new insurance product, and market penetration, whilst growing, remains low vis-à-vis other forms of business insurance (Rafferty, 2021). The hardening market – a situation where it is challenging for companies to purchase cyber insurance and characterised by limited policy offerings and high policy requirements – may have held back the rate of growth in market penetration. The limited penetration means that there is a dearth of data on the scale of the risk and the tolerability of ex-

posure (Nurse et al., 2020; Rivero, 2021; Smith, 2021), but it has been accepted, even prior to the hardening of the market, that pricing has always been the most complex challenge in the market (Harvey 2022).

Secondly, cyber threats are dynamic (Buchanan, 2016). The target surface area that ransomware gangs – amongst other cyber criminals – can exploit continues to expand in breadth and depth. This also necessitates that cyber security practices need to evolve, potentially over short periods of time. At the same time, ransomware gangs continue to finesse their operations, particularly in the critical effort of identifying the Achilles' heel of their victim in order to leverage the likelihood of a ransom payment. This evolution of the ransomware risk is aptly demonstrated by the rapid rise and normalising of 'double extortion' practices (Buckley, 2021). Some ransomware groups have also diversified their approach to drawing revenue from their malware. For instance, 'ransomware as a service' increases the potential to draw upon economies of scale (Davidson, 2021).

Compounding the duality of a dearth of data and an evolving cyber risk is the scope for a singular cyber event to impact multiple insureds. An unappetising feature of cyber risk – including ransomware – is that they have potential scope to be 'systemic', rather than simply attritional. Ergo, a supplier of IT services or software packages may be targeted and compromised with ransomware, with a knock-on impact upon many organisations laterally and/or vertically, all over the world. For instance, in May 2021, the cloud hosting provider Swiss Cloud was reported to have been affected by a ransomware attack, impacting clients including the payroll firm, Sage (Cimpanu, 2021). In July 2021, Kaseya, a provider of remote management software, was successfully attacked with ransomware. This had significant impact on businesses and organisations reliant on Kaseya software; for example, forcing the closure of 800 Co-Op supermarket sites in Sweden due to an inability to open cash registers (Osborne, 2021). Thousands of small organisations may have been affected.

If ransomware exacerbates the scope for cyber risk to be systemic, cyber insurance is potentially viewed by insurers and reinsurers as comparable to other, more established and predictable, forms of systemic risk (Evans, 2020; MacColl et al., 2021). For instance, from a supply-side standpoint, hurricane and earthquake risk may be seen as preferable vis-à-vis cyber risk. Furthermore, the interconnectedness and interoperability of networked devices casts cyber risk in additionally unfavourable terms, because a single ransomware incident could prompt claims across the global market.

2.2. Cyber insurance's impact on ransomware

Within the literature, there appears to be anecdotal evidence that cyber insurance coverage of ransom demands may be fuelling an increase in incidents (MacColl et al., 2021). Ransomware operators have spoken on record about their interest in actively targeting organisations whom they believe, or know, have insurance policies that would enable reimbursement for ransom payments. A LockBit operator, for instance, noted that if they attacked a firm that possessed cyber insurance, a successful payment was "all but guaranteed" (Khodjibaev et al., 2021). A member of the REvil group had been asked in an interview whether their operators specifically favoured organisations holding cyber insurance policies. In response, they replied that such organisations were "one of the tastiest morsels", and even indicated that it was strategic to hack cyber insurers as reconnaissance before conducting ransomware attacks on their clients (Smilyanets, 2021). It is perhaps also of note that insurance firms themselves have been subject to successful ransomware incidents. In March 2021, for instance, hackers successfully targeted CAN Financial and the firm was reported to have paid $40 million in ransom payment (Mehrotra and Turton, 2021). In May 2021, AXA's operations in Thailand, Malaysia, Hong Kong and the Philippines were impacted by an Avaddon ransomware incident (Marzouk, 2021). In both cases, concerns were highlighted that client data could have been vulnerable to theft.

There is a debate as to whether – on balance – the prospect of ransom payment coverage could cause a net harm. Whilst, on paper, the availability of the coverage may either enable a ransom payment when otherwise one would not take place – for instance, because the victim cannot afford it – the coverage of ransom payments in such a scenario could help prevent an organisation from going bankrupt in extremis. Additionally, it is also significant to highlight that whilst cyber insurance penetration has grown markedly in recent years, overall penetration is still low in much of the world, including in developed markets (Dignan, 2021; Abdul Hamid et al., 2022). The UK government's Cyber Security Breaches Survey from 2022 showed that only 43% of UK businesses had some form of cyber insurance policy (DCMS, 2022).

Cyber insurance provides insureds with an in-built support network – both pre-breach and post-breach – that better informs and prepares the organisation in question (Franke, 2017; Woods et al., 2023). This provision of support and experience may be particularly useful for the cyber resilience of smaller insureds. As Eling et al. have argued, not only are there economies of scale with respect to organisational cyber security, but the costs of cyber incidents are also disproportionately expensive with respect to smaller organisations (Eling et al., 2022). Smaller organisations are also less likely to have pre-established – and entrenched – cyber security practices across a large, complex system of networks; they may therefore be more accommodating of recommendations (Abraham and Schwarcz, 2021), dependant on the implementation cost.

Reflecting on the positive-or-negative debate, Logue and Shniderman suggested that "it is, at the very least, too early to declare that ransomware insurance is a net negative for society" (Logue and Shniderman, 2021). A recent report, surveying 5600 professionals in mid-sized organisations (300 of which were in the UK) across 31 countries, noted that organisations that had been impacted by ransomware in the prior year were much more likely to have insurance in the present than those that had avoided becoming victims. 89% of recent victims globally had cyber insurance, whilst only 70% of non-victims had coverage (Sophos, 2022). As the report highlights, "the cause and effect is not clear here"; victims may acquire insurance in the aftermath of an incident, adversaries may be preferentially targeting organisations with insurance, or organisations may be purchasing insurance to pre-emptively financially offset vulnerabilities in their systems (Sophos, 2022).

Ultimately, whilst there is some anecdotal evidence, as presented above, that suggests that ransomware gangs preferentially target insured organisations, this will only be one element of the cost-benefit analysis that factors into the targeting decision-making process. Fundamentally, with ransomware gangs seeking the greatest ransom payment from the least effort – and risk – in conducting the breach and negotiating the demand (Palmer, 2022), the standard of the prospective victims' cyber security remains a significant factor. Here, too, cyber insurance may play a role. In principle, this could be either a negative or positive role. For instance, it is theoretically possible that the financial coverage of ransomware incident response – and provision of support teams – could encourage a moral hazard effect, wherein organisations who have coverage for ransomware incidents may feel less pressure to invest stringently in risk mitigation strategies by improving their cyber security (Bailey, 2014). If this were demonstrably the case, this would suggest that cyber insurance coverage of ransomware incidents could have the potential to constrain what would otherwise be a natural economic incentive to improve cyber security

practices to reduce the likelihood of a costly incident occurring. It is not, however, clear from the literature that there is a demonstrable moral hazard effect in relation to cyber insurance.

Early research has not demonstrated that such a moral hazard is present (Bolot and Lelarge, 2009). More recent research has corroborated this. MacColl et al. (2021), for instance, concurred with prior assessments that a clear moral hazard effect could not be discerned with respect to cyber insurance policies.

It is also difficult to marry the principle of the moral hazard effect with the nature of the hardening cyber insurance market. A MunichRe article highlighted the hardening market as a mutual positive in light of the realities of cyber risk, noting that "ultimately, everyone shares the same goal: mitigating a cyberattack through better cybersecurity governance and investment in controls. Without these corrective actions, insurers could be forced to exit the market entirely due to large losses, reducing options for insureds in the long-term" (Cho, 2021). Recent data may indicate that the percentage of organisations paying demanded ransoms has declined, potentially linked to improvements in crucial cyber security practices such as secure backup systems (Bloomberg, 2022).

The state of the industry can also be viewed through current events. At a recent cyber insurance event, a large broker highlighted five key cyber security controls that they required from prospective insureds before they would engage in discussion of a policy. These controls were, respectively: MFA for privileged access; endpoint detection and response (EDR); encrypted and tested backups; privileged access management; and email filtering (Lawton, 2022a). Seven additional controls were regarded as crucial, but the broker indicated willingness to submit a policy to underwriters if some of these were not fully in place. Whilst we do not claim this to be representative, it is noted that MFA, backup solutions and EDR are widely cited as crucial controls in the mitigation of the likelihood of a ransomware or other cyber breach; these appear to be most-demanded by insurers (Edmundson, 2021).

As it relates to the continued influence of insurance on security, and by extension the ability to mitigate the impact of the ransomware threat, the hardening insurance market may reduce the accessibility and, in lockstep, the utility of insurance. This has been noted in the UK: the most-recent UK Cyber Breaches Survey noted that "in previous years organisations have mentioned protection against ransomware … as a key reason for getting insurance. However, this year it was mentioned that this had become more difficult with insurance companies raising premiums or not being able to cover ransoms at all" (Zank, 2022; DCMS, 2022). This is significant and highlights the complex interplay between insurance and security.

In summary, the convergence of ransomware and cyber insurance is in a process of flux, propagated by a rise in the severity of ransomware incidents. Cyber-risk has been cited as a greater risk to insurers than pandemics and natural disasters (Allianz, 2022). The long-term viability of cyber insurance will depend on an equilibrium that supports sufficient profitability for insurers whilst still meaningfully addressing organisational cyber risk, including ransomware. From our review, it is not yet clear whether ransomware coverage can fit within this equilibrium, nor whether the market can support greater penetration, accommodating more insureds. Of the 300 UK mid-sized firms surveyed in the Sophos State of Ransomware 2022 report (Sophos, 2022), 42% stated that ransomware coverage was part of their insurance policy; 35% held insurance with exclusions or exceptions. Prospective insureds can opt to remove coverage for ransomware incidents to reduce their premium (Lawton, 2022b). Even with this knowledge, however, it is difficult to generalise about all policies, even within the UK. Different policies may include different forms of exclusions; again, turning to the Sophos report, globally, it seems like payment of clean-up costs are more likely to be made than reimbursements for ransom payments (77% of respondents received reimbursement for clean-up costs, compared with 40% that received it for the ransom). Whilst the global cyber insurance market has exhibited hardening, there are likely to be divergences in the specifics of insurance policies between individual insureds, insurers, and jurisdictions; for instance, an absence of ransom coverage in Japan (Pain and Noordhoek, 2022). On balance, cyber insurance may be a well-placed facilitator for some of the solutions that could alleviate net harms presented by ransomware. Ergo, greater market penetration may carry societal or organisational-resiliency benefits. Importantly, at the same time, ransomware itself may be a threat that degrades the very viability of cyber insurance products. Given the immediate challenges presented by the convergence of ransomware and cyber insurance products, this is a prescient area of research for industry, academia and policymakers.

3. Methodology

To identify recent trends with respect to ransomware, cyber insurance and organisational cyber resilience in the UK and thereby answer our research question, we developed a methodology grounded in close interaction with key stakeholders and a set of robust qualitative data gathering and analysis techniques. Semi-structured interviews were performed between September 2021 and February 2022, following the receipt of ethical approval from the University of Kent's ethics review board. Semi-structured interviews allow for a level of interaction with participants that can generate significantly more detailed insights than the broad-brush approach of a survey, for example. In total, there were 65 interviewees, sourced initially from the network of the authors, and subsequently, using snowball selection. We also reached out to several professionals who had authored industry and academic articles on the topic of ransomware and insurance.

Interviewees were chosen for their expertise in either the selling or purchasing of cyber insurance products, the policy aspects around such insurance, or because of involvement in the process of ransomware and other cyber security crisis management within or directly relating to the UK market, and were spread amongst the UK, continental Europe, Bermuda and the US. For a full breakdown of participants by type, see Table 1. In order to ensure a level of candour from participants willing to undertake the interview process, all responses were anonymised. One participant agreed to discuss their experience of being the victim of a ransomware attack: in line with Connolly et al. we found it hard to find other victims willing to speak candidly, even under conditions of anonymity (Connolly et al., 2020).

An interview protocol was prepared by the researchers at the start of the interview process. As a result of the semi-structured nature of the interview process, not all questions were posed to all participants in every instance, in favour of allowing participants to focus on their area of expertise and interest. Questions were always asked around the participant's perception of the state of the cyber insurance market, and any changes they had seen in practices in the last few years. Participants were also asked to reflect on the positive and negative impacts of any such changes, and whether they believed the advent of ransomware had played a role in those changes. A series of questions were posed pertaining directly to cyber insurance and ransomware. For instance, queries related to roles and experiences around handling ransomware incidents (with particular focus on the role of the insurance industry), how the insurance industry is dealing with ransomware, and the extent to which insurance could help mitigate the threat of ransomware, particularly its impacts. The interviews concluded with questions on insurance's coverage of ransom payments, such as whether interviewees believed, or had seen evidence, of insureds

Table 1
Interview Participants by Profession.

Category	Role/type of organisation	Count
Insurance industry (II)	Cyber insurance broker	5
	Cyber insurance claims	3
	Cyber insurance executive	3
	Cyber insurance underwriter	10
	Cyber reinsurance executive	1
	Cyber reinsurance underwriter	1
	Cyber risk management services	2
	Industry Association	3
	Cyber risk analytics	2
Cyber security (CS)	Cyber security consultant	4
	Cyber threat intelligence	3
	Digital Forensics and Incident Response (DFIR)	9
	Public policy	1
	Ransomware recovery	1
Professional services (PS)	Breach counsel	2
	Insurance lawyer	1
Government (GT)	Cyber policy	3
	Incident management	1
Insurance purchasing organisations (PO)	Defence	1
	Financial services	1
	Local government	2
	Technology	2
	Transport	1
Law enforcement (LE)	International law enforcement agency	1
	National law enforcement agency	1
Academia (AC)	Academic	1

Table 2
Workshop Participants by Profession.

Category	Role/type of organisation	Count
Insurance Industry (II)	Cyber insurance broker	6
	Cyber insurance claims	4
	Cyber insurance executive	2
	Cyber insurance underwriter	4
	Cyber risk management consultant	2
	Industry Association representative	2
Cyber security (CS)	Business development (focus on insurance)	1
	Cyber security consultant	2
	Cyber threat intelligence consultant	2
	DFIR consultant	8
	Public policy	1
Professional services (PS)	Breach counsel	3
	Insurance lawyer	1
Government (GT)	Cyber policy	4
	Incident management	1
Insurance Purchasing organisations (PO)	Financial services	1
Law enforcement (LE)	International law enforcement agency	1
	National law enforcement agency	1
	Regional police	2
Academia (AC)	Academic	1

being more likely to pay ransoms, or not, and if cyber insurance has incentivised more ransomware attacks. For the interview protocol, see Appendix A.

The interviews were audio recorded and transcribed, with any identifying features as to the individual or organisations removed. The analysis of the transcripts was conducted using the principles of thematic analysis (Braun and Clarke, 2006). Such a method allows for the investigation of themes across interviews, allowing for certain amounts of flexibility in the theoretical stance taken by the researchers. Like other qualitative studies in this area (Catota et al., 2019), the process of agreeing the final code book took several steps, as a recognition of the number and diversity of participants and the broad range of topics covered within the interview process. Firstly, having read through the transcripts, one researcher performed an analysis of three transcripts to produce an initial code book. This code book was then discussed and agreed between the researchers, before being taken by two researchers to code twenty-one further transcripts. At this point, the code book was discussed and expanded based upon the findings of the two researchers in these twenty-four transcripts. Subsequently, all the interview transcripts were coded deductively using this second version of the code book. The full code book can be found in Appendix B; for clarity, given deductive nature of the coding process, Appendix B also reflects the mapping of initial codes to the themes addressed in this article.

At this point, the key findings of the interviews were subsequently brought to a workshop to discuss and confirm the themes that had arisen from the primary analysis of the interview transcripts (in keeping with processes in, for example, Hadan et al. (2021)). The workshop had 49 participants in total, comprising 18 of the original interview participants, and 31 new participants (who had not been interviewed previously). We convened the workshop over Zoom in mid-February 2022 using four breakout rooms, each with a mixture of previously interviewed and new participants, to discuss, corroborate or refine the initial findings over the period of one hour. The themes and provocations for each of the sub-groups can be found in Appendix C. The comments from this review and discussion process, both audio and chat logs, were then transcribed and included with the original interview transcripts. As no substantial changes were required as a result of the deliberations of the workshop, the code book was not altered for this final round of coding and analysis.

As will be evident in the results that follow, it was very much the case that those themes and points raised by interviewees were agreed with and echoed by workshop participants; as such, in the results that follow, quotes from both sets of participants are used interchangeably.

All transcripts were coded by two researchers, using qualitative data analysis software (NVivo, version 1.6). Following the inclusion and coding of the workshop transcripts, the two researchers then compared their findings once, and resolved significant differences within their coding. The inter-rater reliability was calculated using Cohen's *kappa*. The score was 0.73 which is considered to show substantial agreement between coders (Bryman, 2016).

In the results section that follows, participants will be referred to in the following format: Interview participants will be referred to by their shortened category label (PS, LE etc.) and then a number based upon the order in which the participants in the category were interviewed. For example, the third interviewed participant in the Government category will be referred to as GT3. The same approach is taken with workshop participants, with the inclusion of "W" at the start of their category label. In this case, participants are numbered based upon the order in which they were captured as speaking in the workshop. For example, the second Insurance Industry participant to speak will be referred to as W-II2. Additionally, in some circumstances, where necessary for further understanding, interviewees' specific role/type of organisation will also be provided.

4. Results

The research aims to critically investigate the question: is cyber insurance helping to mitigate the threat of ransomware, particularly its impacts? Three overarching themes arose from the analysis of the data corpus relating to this question. Each of these themes – the accessibility of cyber insurance, cyber insurance and mini-

mum security practices, and the perceived value of cyber insurance with respect to mitigating the impact of the ransomware threat – are explored in depth below. The themes form part of a necessary whole to understand not only how cyber insurance could possibly play a part in an insured, or potentially insured's, organisation's toolkit against ransomware, but also where cyber insurance, as a tool, may face limitations in what it can hope to achieve.

4.1. Accessibility of cyber insurance

All interviewees and workshop participants agreed that there had been a profound hardening of the cyber insurance market in the UK and globally, particularly from 2020. Many interviewees suggested that the complexities of dealing with ransomware attacks had caused a need for a significant adjustment of the product being offered to insureds as claim rates – and complexities around claim resolution – rose. This has reflected in developments such as increasing premiums, reduced coverage, increased required security controls, as well as, possibly less frequently, co-insurance and sub-limits (II-1; II-4; CS-11; II-9; PS-1; II-11; PS-3; II-17; II-19; II-22; PS-3; W-CS12; W-II14), a finding corroborated by news and industry reporting (Aon, 2022; Lawton, 2022a, 2022b). Interviewees explained that as crude rule of thumb, insureds could be "*paying twice as much for half the cover*" (II-6) year-on-year. Workshop participants backed this up: *"premiums have gone up by roughly 100% over the last year or so*" (W-II20). The cost of insurance policies – and the requirements for purchasing them – are rising and becoming more stringent as ransomware has shown the potential for cyberattacks to cripple insecure organisations through business interruptions, at huge costs to the insurers writing their policies:

> "…what ransomware did to the cyber market was it brought business interruption as an exposure. Not every company in the world would say cyber is one of their top concerns, they would all say business interruption is the number one risk they face. The moment ransomware brought business interruption, the world went crazy." (II-5)

Even as this realisation grows, interviewees and workshop participants were generally in agreement that "*we are not yet seeing too much evidence that the worst is behind us…we're not yet pricing that in*" (II-15). A workshop participant broker put it accordingly: "*when government [action is taken], will there be a market left to backstop?*" (W-II17), a stark reminder of the fact that cyber insurance is not only a lifeline for policyholders, but must also return a profit for those involved in writing it. This was a point raised by many:

> "…cyber insurance books have been on fire for most of the past two years. And they have no choice but to take drastic measures. You look at the pricing change… But the insurers don't have a choice. The insurance companies are in business to make money. And they have to raise the rates to a point where they think they can. And likewise limit coverage." (II-17; also II-21; II-27)

Although most potential and renewing insureds would face increasing controls, restrictions and premium rises in relation to coverage they would be able to purchase, there was suggestion from some, particularly in the UK, that this had not trickled down all the way to the much more "*off the shelf*" insurance products that the smallest organisations would purchase, with limited interrogation as to their security setup (II-18).[1] This may be because the volume of policies written would cover the relatively insignificant costs of acting upon a claim from the smallest organisations: the threat of business interruption or data leak that ransomware may pose is likely very limited where the organisation itself does not have significant infrastructure, turnover or personal data:

> "…if you're insuring a business that turns over £500k a year, there's only so bad it can get, right…say you've paid £1500 for a policy, it's cheaper for [the insurer] to send you a new laptop." (CS-18)

Participants were broadly in agreement, however, that anything larger than the smallest of organisations would likely be noticing price increases and coverage reductions in the UK market at present. As a workshop participant explained though, that was only to be expected in the current market: *"If you're getting cheap premiums now, you've got to question how…what's in the wording that's restricting cover?"* (W-II7). Larger organisations, with insurance policies typically written jointly by several underwriters (in a "tower") were reported to be experiencing a more protracted process in the renewal of policies, in part as a result of the apprehension of underwriters: not implicitly trusting risk-assessments undertaken by others, each underwriter requiring their own risk review be undertaken. A similar apprehension also sees additional checks around risk management being undertaken by the reinsurers involved (II-18). Although the recognition that an insurer's process of managing risk appetites within a portfolio is not unlike that of a fund manager balancing their fund weightings (Franke, 2017), potential insureds seem to be increasingly aware of it in the current market. A purchaser of cyber insurance at a large organisation described recent renewal experiences as:

> "…like Dragon's Den. You prepare a lot of slides about your organisation, its risks, what your cyber security posture looks like, what you're investing in, what it looks like over the next 2–3 years, what insurance cover you're looking for. Most of them walk out, have questions, put half their money away, you wind up with a smaller number of insurers." (PO-4)

As the market has hardened, so certain sectors have moved towards becoming uninsurable. There is a clear business reason for this: *"to write a sector that is heavily, heavily unprofitable, is just going to make your capital go even further away."* (II-7) Such unprofitability arises from a number of different risk profiles: some sectors – such as manufacturing – are regarded as being acutely vulnerable to the risk of business interruption, a threat that ransomware has crystallised in a way not previously considered (II-10; PO-5; II-27), along with insureds with primary business activities involving complex supply chains or cloud or IT solutions. Other sectors – for instance, local government bodies – are regarded as having historically poor levels of cyber security practices. In the UK particularly, this was linked to underinvestment, potentially due to decreased budgets. One broker reported that:

> "…county councils, police authorities…their failure to invest in security over the last couple of years, decades. And insurance has been quite a crutch for them, to be honest. So, the removal of that insurance has been a challenge…we do not write public sector, you know, these aren't areas of interest for us, even with good security." (II-19)

[1] The interviewing team did not direct interviewees towards a particular interpretation of what a micro, small, medium or large-sized business many be, and there are difference between UK and US formal definitions (see Department for International Trade, 2021; US Small Business Administration Office of Advocacy, 2020). As such, definitions between participants from, or working within, differing jurisdictions may have had slightly different parameters when discussing small and larger businesses.

Other potentially uninsurable sectors were highlighted by interviewees, including (but not limited to) airlines (II-4; II-27; PS-3), education (II-4; CS-6; II-10; II-23), public sector (II-10; PS-3), hospitality (II-4; PS-3), healthcare (II-12; II-21), manufacturing (II-22; II-27) and critical national infrastructure (II-4). Prospective clients operating in 'uninsurable sectors' may not be able to get any, or sufficient, cyber insurance coverage even if they are able to demonstrate that they have a comprehensive grasp of their cyber security practices. As one broker indicated:

> ".. those risks, insurers just don't want to pick them up anymore, even when they're best in class [placing new clients in these sectors] this past year, has been nigh on impossible." (II-23)

Given the obvious concerns that having such uninsurable sectors may raise, would it not make sense for the industry to lobby for a government backstop, to avoid catastrophic loss? Participants did not seem convinced that a Pool Re-style reinsurance offering would necessarily be beneficial (Lucas, 2018). Not only would the claim rate be far too high, compared with the claims made in the Pool Re structure, but it may well skew incentives, knowing that the government would have a requirement to step in:

> "…political violence is pretty easy to cover because it doesn't happen that much…If you go cyber… SME, urgh, gets ugly, it's a lot of losses. And then for the big stuff, I don't think they'd be equipped. I think you need to change the risk environment, before you look at just throwing government money at something. Because once you've got a government guaranteed payer, I mean, cheque books open." (PS-4)

It would appear that cyber insurance is increasingly important for insureds as a way of mitigating the impact(s) that ransomware may have – but this importance is reflected in ever-higher barriers to entry and renewal. This suggests that cyber insurance has a mixed ability to mitigate against the realities of ransomware attacks. The hardening of the market highlights the ways in which the pressure from the crippling effects that ransomware can have on the running of organisations had not been appropriately understood, or priced in, historically. Ironically, such hardening should also signal to prospective insureds the increasing need for cyber insurance, precisely as claims rise in the face of escalating cyber risk. It shows the reliance that insureds are placing upon their cyber insurance as a way of dealing with attacks when they occur. As the insurance industry has rallied to understand the risks associated with the significant increase in claims since 2020, so their standards for insuring clients have raised. This leads to the difficult endpoint that some sectors, at present, may be relatively uninsurable, thus unable to mitigate the ransomware impacts through insurance.

4.2. Cyber insurance and minimum cyber security practices

One consequence of the hardening cyber insurance market has been the requirement that prospective insureds meet higher cyber security standards. This directly relates to our research question and the potential positive impact of insurance for the insured in ransomware mitigation. Insurers and reinsurers described how they seek to gain a better understanding of the cyber security footing of prospective insureds, in particular, the extent to which they could stave off potential ransomware attacks. Multiple interviewees recited similar lists of necessary security controls.

> "I'm listing [the controls] out…without any notes in front of me, because it's kind of ingrained into an underwriter's head now, that all these controls are really important to mitigate or prevent or reduce the cost of a ransomware attack." (II-4)

The basket of security controls that are now demanded could be said to look similar to general governmental guidance.[2] So why do insurers not simply mandate adherence to one or other of these guides or standards of best practice? Participants were of the view that these were necessary, but not sufficient, steps to show robust cyber security measures, except, perhaps, in the smallest of organisations. In the UK, Cyber Essentials is the recognised governmental standard.[3] Participants articulated, however, that this standard is too basic and/or outdated for organisations above SME level (II-18; II-19; II-23; CS-16).[4]

> "I had a UK retailer recently [looking to gain insurance], a fairly sizeable company, but when it comes to…the controls they were describing, they were exceptionally basic…'Oh yes, we follow password guidance from the National Cyber Security Centre' [and I said] 'Yes, but I was asking you about privilege access management…'." (W-II5)

Insurers were also reticent to require potential insureds to follow certification schemes from organisations based outside of the UK, such as NIST, because this could impact the potential client base (CS-9; II-25). Standards were not felt to be specific enough to give any ideas as to how the organisation in front of them asking for insurance would look or behave:

> "…we need a way of certification that is thematic, or broad brush enough that it covers four or five dynamics of a company's policy posture … but [there] needs to be gradation in it; we cannot have this binary [of] 'You meet a standard, yay!'." (II-9)

As such, a key aspect of requirements being handed to prospective insureds are instead drawn from the combined experience of underwriters, claims handlers and breach responders, based upon an insurer's handling of prior claims (PO-3, II-24). By far, the most-commonly demanded security controls were MFA – either on all accounts or on remote access accounts[5] – network segmentation, secure offline backups, regular patching cadence, remote desktop protocol (RDP) access control, and endpoint detection and response (EDR) solutions (II-1; CS-1; CS-4; II-2; II-4; II-8; CS-11; II-10; II-11; II-12; II-14; PO-3; II-17; II-19; II-20; II-22; II-23; II-25; II-26; II-27; CS-16; II-28; W-II7; W-II10; W-II12; W-PO1).

How, then, do insurers work to get the information that they consider necessary to understand a prospective insured's security footing? Questionnaires and external scans were mentioned as being particularly popular; yet both were described by some as having considerable flaws. The particular methods used – and weighting applied to those methods – varied between insurers. As one interviewee noted, "*I don't think everybody's using the same tool suite, or the same philosophy*" (PS-4). In the workshop, one participant working for a purchasing organisation explained the frustration their organisation felt when their experience was *"a controls culture…tick box, great everything is fine…"*. They went on to talk about their experience of describing their backup processes: "*[the insurers] don't really care how you've managed [it]…or that somehow there's a connection so it's not really offline…that's kind of a dangerous thing*" (W-PO1).

[2] Such as that put out by national and international cyber security bodies, such as the UK's National Cyber Security Centre (NCSC), or the US' National Institute of Standards and Technology (NIST).

[3] The NCSC's programme to help organisations improve basic cyber security measures. For more see (NCSC, no date)

[4] It should be noted that some elements of Cyber Essentials were updated shortly after these interviews were performed.

[5] Arguably a significant distinction – particularly in the case of large organisations.

Concerns were raised about the utility of external scanning tools. One cyber security stakeholder likened these to credit-rating checks; attractive because of their simplicity and relative ease, but "superficial" for the same reason (CS-3); "*…from a practitioner's perspective, I wouldn't trust them at all, because it's so passive and removed that it doesn't really tell you much*" (CS-10). It was considered that it might, at best, highlight low-hanging fruit – and at worst, may reduce the insurer's credibility by showing the lack of knowledge of the limitations of the scans themselves. An experienced cyber security consultant shared a story exploring how external vulnerability scanning highlighted a lack of insurer knowledge in their business model:

> "…we were scanned by one of the well-known organisations, who then pinged a note to our CTO to go 'Oh my God, you're super high risk of being ransomware-d!' And he went…'Yes, what you discovered was our training network that was deliberately left open for our training people to go and train on. And you completely missed everything else.'" (CS-6)

Insurers agreed that false positives were standard with external scanning, and that red flags would be confirmed as a false positive with a conversation with the prospective insured (II-28). It was also noted that whilst they used an external scanning tool as part of their underwriting procedure, this was "*generally only to spot whether there's any massive red flags*"; rather, the bulk of the risk assessment would be derived through the questionnaire (II-14).

The efficacy of questionnaires was queried by participants both in the interviews and workshops; as highlighted in the previous section, all participants involved in the underwriting process were now insisting on their own questionnaires (PO-3). Furthermore, despite insurers using separate questionnaires for ransomware (II-11; II-16; II-26), they were described as being too "binary" to capture the finesse or nuance of contemporary cyber security and ransomware risk (II-4; II-10; PO-4; CS-14; PO-5; CS-18), an argument echoing that made in Sales (2013). As a broker put it in the workshop: *"We just recently redid an application form, because we were fed up with the 15 different versions that were told had to be complied with by the market, so we made one that basically did everything in one place."* (W-II7). Not only might insureds have to answer "*the same question by nine different teams and in nine different ways*" (II-19; also II-27), but questions, poorly posed, could lead to ineffective, yet seemingly "correct" answers. One interviewee referenced an example of insurer who only offered policies to clients with backup procedures in place – policing this through questionnaires – but that whilst one of the clients did produce backups, they had not taken a backup for eighteen months (II-9). For the interviewee, this highlighted the importance of internal policies and internal cyber security culture, rather than system security per se (II-9). A lack of cyber security knowledge, too, can be covered up with a "correct" answer on a questionnaire, as one cyber security stakeholder described:

> "…we did a ransomware risk assessment for a company. They've got EDR [Endpoint Detection and Response] everywhere it's all wonderful, really good, we did some really simple tests, [following the tests we realised] we've got an issue here…we'd gone onto one of their servers and [were able to] run Mimikatz…Completely went like "What the hell's happened here?!" Turns out no one had ever taken their EDR out of learning mode and [put it] into blocking mode. It just never happened. They're insured and I know on their form they said yeah we've got EDR everywhere, because the form says have you got it or not, it doesn't say is it configured properly." (CS-18)

The challenges of assessing the risk, assessing the measures to mitigate the risk, and assessing the assessment methods, place insurers in a challenging position. An incident responder described this accordingly:

> "…insurers being able to effectively price their risk – it's really, really hard, and insurers are also not doing a good job of it despite how hard it is of measuring the risk…doing a security assessment, you ask any security consultant out there, they'll struggle to do a reasonable security assessment for less than [£15,000]. Now the price of a cyber policy for most organisations isn't much more than that, so that doesn't work…" (CS-9)

Many participants noted that there is another issue for insurers: the "shortage of skills" (II7) of those responsible for assessing the risk.

> "…I don't think all underwriting claims teams have the knowledge, the capability, to understand this risk properly. They don't have specialists…it's either the clever grad that wants to get in because this is a growing space, or its someone that isn't good at other things and they been ousted into this space… and that leaves these problems." (CS-9)

This leads to difficulties in those fundamental aspects of underwriting in particular – the modelling and balancing of risks to achieve a palatable overall portfolio. In more established insurance lines, participants described how modelling was easily carried out by people with significant "*histor[ical data] and…PhDs*" (II-9), both of which are not as available for cyber risk, leaving "a skills gap", meaning that the "*mental map isn't there*" (II-9).

Even with the right sort of questions in place, there remains the question of whether the relative novelty of cyber as a class means that those underwriters dealing with the answers "don't have the history and the experience in it…do they know what to do with the [answers to the questionnaires]?" (II-13)

The inevitable transfer of the same small group of knowledgeable participants from firm to firm "because they don't know where to get people from" (CS-14) leads to a lack of thinking *"outside the box"* (CS-14) in terms of approaching the risk. The novelty and size of the market, however, also has led to firms giving significant exposure to relatively inexperienced underwriters:

> "… you see some [underwriters] come in, they've just been underwriting liability a year, and they've been given £10 million line down to put down – some of the older underwriters are horrified – the limited experience in their mind, and the amount of money they're being given to write…it's the nature of the beast – there's not enough experience to go around." (II-18)

And so, in the face of ever-increasing losses, it must be noted that a primary driving force for insurers behind the raising of minimum cyber security practices was the desire to protect profitability – and sustainability – of cyber insurance. In this sense, insurers had a financial interest in the raising of cyber security to: (a) reduce the likelihood of ransomware infecting their insureds' systems; and (b) reduce the costs of ransomware incidents, were they to occur. Given the significant leverage that insurers have over those wanting to be insured, this necessarily has forced an adoption of those measures that the insurance industry has decided should be in place in order to gain coverage. Some organisations were reported to be considering whether self-insurance against cyber risk may be more palatable in the face of sky-high premiums, but this is neither feasible nor realistic for organisations who lack significant financial reserves (CS-8; II-6; PO-4; II-23). This leverage may end up with more organisations having better security footing, and is certainly more likely to effect change than cyber secu-

rity solution vendors, on the whole: "*…customers ultimately aren't going to do anything unless they know it's going to be reimbursed*" (II-2). Another underwriter stated that they were "*making the client think more about their security. We're trying to force those minimum standards to increase, so that the losses come down.*" (II-8)

The speed at which the cyber threat to insureds evolves is far greater than the time between renewals. How did insurers hope to mitigate the impact of new threats arising to insured during a policy period? Underwriters discussed the possibility of using specific triggers to require the insured to act within a specific time frame, or have their coverage limited. It was noted that purposefully used regular insured surface scans and detailed provision of threat intelligence – already offered by many insurers – could help to target such risks specifically and quickly (W-II9). One example given was that high-end common vulnerabilities and exposures (CVEs) could fall under endorsements, as a way of limiting the insurer's exposure to threats that were not known about at the time of writing the policy. Should an insurer identify a vulnerability in an existing insured's system, and inform them of the vulnerability, they could then give them a time limit to patch it or risk losing all or partial coverage if that particular vulnerability is exploited by hackers (II-8). Coverage could lapse fully if the vulnerability is not patched within a stated period (II-8).

Such a tightening of requirements may be driven by a desire to protect profitability, but it also drives towards higher cyber security standards: in this respect, it must be considered that cyber insurance will mitigate impact of the ransomware threat simply by ensuring that insureds take more steps to protect themselves. Some interviewees recognised that it took a shock to the system – the shock provided by the threat of sustained losses from claims relating to ransomware – to stop cyber insurance being priced inappropriately, with the potential risks posed by an online world being misunderstood. The way to reducing these losses has, despite being significantly more expensive than ever before to hold such policies, required potential insureds to evidence their cyber security practices in ways never previously considered.

4.3. Perceived value of cyber insurance with respect to mitigating the impact of the ransomware threat

The previous themes considered how, by raising the barriers to entry, cyber insurance should clearly be helping insured organisations to mitigate the impact of ransomware attacks. But is this as objectively true as one might imagine? This theme focuses specifically on the value as perceived by the study's participants. Ransomware has, in effect, prompted a recalibration of risk-assessing cyber threats to organisations; it is regarded as the "next evolution" of acute cyber risk (PS-4). A consistent theme in the interviews was that the addition of potentially severe business interruption in combination with the often severe, but more widely understood, data leakage should cause organisations of all sizes to be fearful:

> "…the difference is if you go back 4–5 years ago, losses from ransomware didn't exist…one of the reasons why we struggled to sell the product, because people didn't think they had much exposure, it was all very much a data exposure, and if you didn't have data, you didn't buy the product." (II-8)

Whilst it was clear that business interruption coverage is, "*the thing clients need [in a cyber insurance policy] … that keeps them running as an entity*" (II-8), feelings were mixed as to the threat that data exfiltration poses to organisations. Despite data breaches becoming more routine, every time data is stolen it can "*feel as grave as the business interruption*" (PO-6). Quite aside from the increased regulatory obligations associated with the disclosure of data breaches – it can never be concretely ascertained by the victim where the data has ended up; if it has been leaked online, this may lead to significant legal fees to secure injunctions (W-PS3). There were mixed opinions upon whether data exfiltration would more likely cause an organisation to pay a ransom. "*…we have had so many clients that have decided we're going to pay that ransom to avoid that data being released. I would say 80% of the time the data gets leaked anyway, even if you pay the ransom*" (II-5). Participants suggested that on balance, it was better to not pay the ransom to prevent data leakage, because the victim could be hit with a secondary impact via a reputational hit; both for the exposure of the data and for the payment to a criminal entity (II-5; also CS-11; II-28).

One of the core aspects that a cyber insurance policy provides to firms that may otherwise not have the capacity is resources, in the time of an attack. Ranging from lawyers, to digital forensic specialists, recovery teams, data breach and data protection specialists, PR teams and negotiators, these groups of experts are either brought in externally (as part of a "panel" of such experts) by insurers at the moment the insured needs the support, or, in some cases, may be a specialist part of the insurance firm itself. This support network could be particularly useful for smaller insureds:

> "the smaller the entity, the more they need those services because they don't know how to fix an issue…they don't have a hundred people in IT who can advise them who to speak to, to help fix it…we have it there for when clients need it." (II-8)

This was echoed by participants in the workshop:

> "[previous participants were talking about] the difference between insuring recovery efforts and costs and [just] paying [the] insurance [premium]…This only occurred to me now and is obvious to everyone else but that seems like quite a powerful distinction to make." (W-CS9)

The centralised nature of the response allowed for proactive crisis management, particularly in more complex situations. A legal professional described this accordingly, suggesting that whilst there was variation:

> "…if you've got the messiest types of ransomware incidents that have run over weeks and it's knocked out national level companies, the best situation would be: each day you have a main management call where you have the client, internal stakeholders, you'd have your forensics and you'd have your PR, [and] the breach coach, typically chair[s] those meetings. Everyone then goes off and does their own work stream, so the forensics are dealing with the IT leads day to day. PR are dealing with the comms guys day to day, so everything's not coming through us [the insurer] but once we've kind of set things up, in some respects we are the gatekeepers … but by and large then everyone goes away and does their own thing and then reconvenes, if you see what I mean." (PS-3)

Given the sheer number of specialised roles that may be required to manage a post-ransomware recovery, it is reasonable to ask two questions: where do insurers fit in, and also, is it not just cheaper for insurers to promote paying the ransom, rather than footing the cost for all these professionals?

It was clear that – although insurers may, to some extent, be involved in deciding who may be in the room, given their ability to choose who is part of the initial panel that is put together – they are largely not involved in decision-making day-to-day. The removal of insurers from the hands-on decision-making process during an incident meant that insurers were not generally in a posi-

tion to push for particular remediation approaches. A ransomware recovery specialist detailed how insurers were "*not really in the room, if you will, when these decisions or discussions are made…typically the insurance policy require, you know, some sort of pre-approval before a ransom is paid…the insurance company has to at least acknowledge it, and give consent or waive consent*" (CS-13). This was further corroborated by another incident responder, who described how:

> "the general flow is the breach coach or claims person reaches out to validate availability and capacity and clear conflicts, following that there'll be a kick-off call with the client where the claims officer will attend. And that's the verb I use rather than participate. Often times they're there just for specific questions and to sort of make sure that it all happen. And if everything goes smoothly, there's really no involvement from the claims team other than a weekly budget update." (CS-15)

The insurer, thus, may be informed to the extent necessary as per the terms of the policy in question. An interviewee from a consultancy firm involved in incident response noted that after being contacted by the panel-forming entity – often an insurer:

> "…we end up getting into a situation where there's a meeting, we do a scoping call, we understand what's happened. And then we basically go away and put together a scope of work to recommend how we can help the client, that side of the work does get scrutinised by the insurer, it's not an open book, we can't go and rebuild the client's environment and all that stuff, there's very strict rules or unwritten rules about what goes into that." (CS-16)

That the insurer is rarely involved in decision-making, so much as essentially being there to approve the spend, is an important aspect of approaching the debate as to whether the existence of cyber insurance could be promoting the payment of ransoms. This view is based on a perception that in some cases, payment of a demanded ransom may be the cheapest option available to the victim.

Some interviewees raised this concern; particularly interviewees from government and law enforcement. For instance, one law enforcement interviewee speculated that: "*I don't think we know…instincts would say that I think if you are insured against it, you are probably more likely to pay…I think the data on this is poor…if you have insurance you're more likely to pay because it makes more sense for you as a business*" (LE-1). A civil service interviewee suggested that insurers "*normalise the payment of ransoms. It's turned into sort of standard business practice*" (GT-4). Furthermore, an international law enforcement interviewee expressed the view that insurance firms would prefer their clients pay a ransom if it was cheaper than the cost rebuilding damaged infrastructure, although they acknowledged that "*we don't have the data to say that*" (LE-2). Additionally, the interviewee also noted that:

> "…what we certainly see that a lot of criminals now use the fact that organisations have insurance…makes them more likely a target…" (LE-2)

This is a sentiment borne out in media interviews with ransomware operatives: "Conti prefers targets that have cyber insurance in place as they offer a higher chance of a successful payday … some of Conti's targets are prioritised over others because they have cyber insurance" (Check Point Research, 2022), see also (Khodjibaev et al., 2021; Smilyanets, 2021). Unsurprisingly, those in the industry did not consider paying a ransom was the panacea that it might seem at first pass:

> "All the professions I've ever worked with do everything they can to try and avoid a payment being made, whereas it seems the court of popular opinion is oh this is really easy for us, let's just pay the ransom and we'll move on. This is absolute nonsense because you still end up rebuilding the environments, you still end up dealing with notifications and all the legal fall out, and all we've done is pay the ransom on top of that." (W-II12)

That said, there was also recognition from inside the insurance industry that the creation of panels to process such events may well facilitate ransom payments where this may well not have otherwise happened:

> "Most organisations, if there wasn't a market for the negotiators as well, would have no ready access to Bitcoin and it'd take them weeks and months to get all of the financing through…whereas now it's a legitimate bank transfer and somebody else deals with that side. It's that combination of those two things which has created the perfect storm of actors knowing they can get huge pay days, very quickly and with very little pushback." (CS-12)

A risk analytics specialist, discussing the propensity to pay a ransom, suggested that it was:

> "…probably 50/50, right…obviously no-one from the insurance industry really wants to go on the record and say, clearly it has amplified this. It clearly has. But, for everybody in that value chain, it has become a business decision…to pay or not to pay, as long as there is a high probability of recovery, you pay. The only way that you stop paying is to legally disincentivise payment." (II-9)

To complement these perspectives, a breach counsel interviewee suggested that:

> "…there's definitely a difference of approach by insurers across the market. Some have more of a set position in relation to ransoms, but I think probably the one thing that unifies them all is it is ultimately the decision of the insured to pay a ransom. The other thing that I think probably unifies them is they're very careful to try and educate insureds as to their actual experience of what happens if you do pay a ransom and the pros and the cons of it. So they're giving the insureds all the information that they need to be able to make that decision." (PS-4)

An interviewee from a large insured organisation noted their firm's finances were such that they would not necessarily need to draw on a cyber insurance policy when deciding whether or not to pay a demanded ransom (PO-2). They noted that sourcing the payment of a ransom from an insurance policy may make the decision more palatable for the leadership, but that the existence of insurance was unlikely to be a decisive factor (PO-2).

This is the key argument for the importance of cyber insurance: whilst not all organisations would have the funds to pay a ransom as the one mentioned above, it does provide more options as to solving the issue when it occurs. An underwriter explained this accordingly:

> "…if they were uninsured, they just wouldn't have the options that we're giving them, potentially they wouldn't have access to the same level of expertise to try to recover their data, to access publicly available decryption keys if that is the case and to work through all of that process, to get to the point where it is the last option to pay the ransom, so with our help I think it's a lot more likely that the ransom wouldn't be paid." (II-16)

Another insurance stakeholder concurred, noting that the support offered by the insurance "*means they've got other options than*

just paying the ransom. It actually makes it less likely that they'd pay" (II-18). An executive of a cyber insurance firm emphasised:

> "the vast majority of times, clients elect not to pay because they have the financial security because that's taken care of by insurance, they don't have to worry about litigation because that's taken care of by insurance, they have another option…that's what I mean by having other options, financially they don't have to worry about a potentially business ending event." (W-II12)

On top of the ability to offer services, participants noted the accrued knowledge of ransomware operatives that those firms working on a panel could provide to the insured in the event of an attack. This knowledge would be particularly important in explaining the risk of even considering paying a ransom. As one claims professional put it:

> "Sometimes the decryption key is a much faster means of recovery even if you had backups. I know security experts will say there's often really crap keys out there, and that's also true. [This is] something that the best ransomware negotiation experts and other technical experts can often opine on in the middle of the event." (II-1)

One cyber security consultant recalled instances where decryption keys, once obtained, contained coding errors, or, even worse, could not decrypt because of some issue on the encryption side (CS-6). This outcome would lead to a fresh set of concerns: was the inability to use the key intentional? Did the purchase of the key add the victim to *"the sucker list, where they'll get hit again? Have they guaranteed that there's nobody still on the network…They could decrypt and then re-encrypt all over again.*" (CS-6).

Despite the risks, participants noted that – even if some insureds would pay the ransom because of, rather than in spite of, their insurance, and even if some ransomware groups used lists of those with insurance to target – the reality remains that cyber insurance has low penetration rates and thus, proportionately, could not be said to be making a significant difference in making ransom payments more palatable when the majority of organisations still did not have coverage:

> "let's not forget that cyber insurance still has very low levels of penetration … so globally less than 15% of businesses, and I would say less than 10% of businesses buy cyber insurance, so it's kind of the tail wagging the dog if you think that the 10% is driving the 90%." (II-2)

In addition, remembering the relatively distanced role that insurers have during an incident, interviewees argued that it is the victims who make a decision as to how they would like to proceed during an incident, and whether or not the ransom should be paid: "*ultimately it's the end client that's deciding on decisions like pay or don't pay*" (II-2) and "*you're going to pay a ransom, that is your decision as a business. We are not going to say pay, we are not going to say don't pay, that's not our call, it's your business, it's your call*" (II-5). However, a common narrative was that the support network provided by insurers were increasingly cognisant of the importance of sanctions compliance checks: this additional scrutiny this required further reduced propensity to pay ransoms (II-1; CS-8; AC-1; CS-9; II-4; II-5; PS-1; II-11; CS-12; II-15; PO-2; II-16; II-18; II-19; II-21; W-II10; W-II12). Insurers, being regulated entities and as such bound by additional standards and scrutiny compared to other actors involved in the restoration process, would not be able to reimburse payments that were made to organisations that were subsequently found to be sanctioned, and similarly would not receive their own reimbursement payment from reinsurers. One workshop participant gave this example of guidance recently given to insurers: "*the Lloyds Market Association put together a guidance note or protocol putting together checks that should be made before a ransom payment is made, so that sets out all the sanctions and the checks that should be made at a fairly granular level.*" (W-PS2)

This finding suggests the importance of the updated guidance with respect to ransomware from OFAC in 2021 (Department of the Treasury, 2021) in ensuring proper sanctions checks throughout the process (II-8; CS-11).

5. Discussion

The responses reflected in the interviews and workshops highlight the difficulty of appraising the role of cyber insurance in terms of mitigating the threat of ransomware, particularly its impacts. The first two themes analysed in the results section – the accessibility of insurance and the increasing cyber security standards needed to get insured – showed that a hardening market presents opportunities for insurers to require higher cyber security standards prior to offering insurance which, appropriately done, will end up with insureds with better cyber reliance. However, hardening markets mean that some organisations cannot, or will not, access insurance at all. This leaves questions over the possibility of using cyber insurance, and thus the insurance industry as a whole, as a way of policing cyber security controls and, by extension, potentially limiting the success of ransomware operations. Participants recalled the difficulty with which the industry, in this moment, seemed to have with the fact that seasoned experts with an ability to understand the cyber security risk and subsequently meaningfully quantify it. Although, the argument may have been made that, ultimately, insurance may end up running the computer security industry (Schneier 2001), the reported state of technical knowledge at present suggests that asking insurance companies to be the arbiters of good cyber security practice is not appropriate at present. As the third theme highlighted, perceptions of the value of the product are disparate, depending upon who is asked the question. The discussion about the bearing of insurers on ransomware is also complicated by polarised stakeholder positions about the options that having an insurance product provides to an insured. These positions highlight the fact that the act of professionalising the process of organisational recovery after a ransomware attack can both be the most beneficial option provided to a firm whilst also making acquiescing to criminal demands easier; but also, that not having insurance may limit an organisation's options down to only those demanded by the ransomware operative.

5.1. Difficulty of using insurance as a way of policing organisational security standards

The interviewed candidates made it clear that if it were not ransomware, there would have been some other threat that would have emerged and made both insurers and insureds take notice. There was a recognition from participants – albeit, perhaps, in hindsight, that both the hardening of the market, and the increase of cyber security hygiene would have happened at some point – and it happened to be prompted by ransomware. The double impact of business interruption and potential uncontrolled data exfiltration requires both strong organisational cyber security strategies, but also robust mitigation strategies when the cyber security fails (Kenneally et al., 2020; Logan et al., 2021). What the hardening of the insurance market in light of the rise of ransomware shows is how reactive the insurance industry has had to be to protect their books (Romanosky et al., 2019; Lerman and

de Vynck, 2021; MacColl et al., 2021; Millman, 2021; Ruel, 2021; (Sophos, 2022); Sheehan, 2022). The sudden hardening of the market could be interpreted in at least two ways. It is possible that the pricing of policies was too cheap before ransomware became a major issue. Alternatively, the movement toward increased pricing could indicate the importance that is now placed on increased understanding and correction of what is needed as a minimum to gain access to appropriate coverage.

Regardless of these interpretations, this reactivity is extremely important for two points. First, it underlines the fact that, whilst insurance may be considered a vital source of risk management in today's society, it is entirely up to the insurer whether or not they will write a policy. If they choose to do so, they determine at what price, and under what terms, they will write it at, based on their own understanding of the risk impact (Smith, 2021; Curtis, 2022). Second, it shows how the insurance industry is (or certainly was) somewhat behind the curve in understanding what robust cyber security standards in organisations should be (Lerman and de Vynck, 2021), in part because of the novelty of the risk and subsequent inability to understand it (Markopoulou, 2021; Cremer et al., 2022). The interviews, as well as a number of industry articles (Jimenez-Sanchez, 2022; Muncaster, 2022; DuChene, 2022) show how this has been exacerbated by a lack of specialist knowledge. Both points raise significant issues in terms of the expectations that it is, arguably, possible to have of the insurance industry when considering the industry's role in mitigating the threat of ransomware.

Indeed, it is possible to consider that whilst the closing of the market to, in some cases, entire sectors, highlights the limitations that cyber insurance can have in mitigating something as profoundly dangerous to organisations as a full-scale ransomware attack, it is important to recognise the importance of the lack of ability to understand the risk fully. In the situation where they appear to be at present, it is hard to expect insurers to be able to ask the right questions – and interpret the answers appropriately – if they do not have the requisite expertise. In this case, at this moment where the "race to the bottom" (Woods and Moore, 2020) has caused significant losses, the subsequent tightening of requirements means that whilst those that can afford to pay premiums and improve their security footing will benefit, those that cannot may see none of that benefit directly. Indirectly they could, of course, should they interact with organisations who have improved their cyber security footing to gain insurance coverage, as explored in Sales (2013). However, given the potential severity of ransomware risk for some organisations – manifested most acutely in terms of business interruption and data breach – without access to capital, some organisations who may survive an incident with cyber insurance coverage may otherwise go bankrupt in its absence (Cowbell, 2020; Woods and Moore, 2020; CNBC, 2021; Knutson, 2021; MacColl et al., 2021). An interesting finding here was that large organisations may be more likely to treat cyber insurance as an 'option' to assist in a severe ransomware breach; this could be due to their size and the reality that they are more likely to have the opportunity to self-insure (Holmes, 2022).

Ransomware is far from the only risk that insurers face that can see enormous losses rack up, yet participants were not keen on the notion that a government backstopped reinsurance fund may be beneficial, a sentiment shared in the literature (Ryan, 2016; Woods and Simpson, 2017; Wolff and Lehr, 2018). Across all cyber insurance products for all organisations, such a scheme absolutely makes no sense. Yet large number of uninsurable sectors are public bodies, with participants describing their lack of funding and expertise as key features behind the lack of insurability. In these cases, lack of a profitable insurance product leads to significant holes in any positive mitigation that insurance products can provide against ransomware.

The raising of minimum security standards, albeit as a result of severe losses, is obviously beneficial for organisations that work to meet those obligations, as their security profile should be raised as a result. The data collected paints a mixed picture as to how straightforward a win this has been. Underwriters and brokers are not cyber security specialists (although some have moved to bring cyber security firms in house; for a recent example, see speciality insurer HSB's acquisition of a cyber security platform from Zeguro (HSB, 2021)). Participants highlighted insufficient screening practices during the policy agreement or renewal phase. The requirements – whilst obviously differing dependant upon the size, industry and organisational setup of a potential insured – remain largely in line with those that cyber security certifications (whether that be comparable to Cyber Essentials for SMEs, or NIST Cybersecurity Framework (CSF) or ISO 27001 certification for larger firms) (ISO, no date; NCSC, no date; NIST no date), have required for a significant period of time (NCSC, 2021; (Sophos, 2022); Lawton, 2022a). Importantly, though, cyber security standards and certifications were largely dismissed as being little more than part of the discussion rather than be taken at face value, with significant further documentation and discussion of practices required by all the insurers (and possibly even reinsurers) involved in writing the policy.

Insurers are de facto acting as policemen to raise standards amongst insureds (Kudale, 2021) – an act that must serve to mitigate the threat of ransomware by virtue of reducing possible attack vectors. Yet, given that they are reliant upon pricing policies based upon their own understanding of risk – which has, arguably, been behind the curve in recent times – it is risky to continue to use them as the arbiter of cyber security standards amongst organisations. Other types of insurance an organisation may be obliged to take out in the UK (such as employers' liability insurance) have a legal basis behind them – that is, the insurance helps the company meet legal objectives.[6] To date, there is no such obligation or legal basis for cyber insurance. This may not be palatable for a number of reasons, least of all the speed with which cyber threats proliferate and evolve. But this would provide an understood basis, set out by government, as to what qualifies as adequate cyber security measures for organisations, as opposed to putting this on the shoulders of the insurance industry, who are not appropriately placed to bear the entirety of the societal risk that cyber threats such as ransomware can pose.

5.2. Differing views of stakeholders as to the mitigating power of insurers

One issue that became apparent during the interview process was the entrenched views that groups of participants appeared to hold about the potential for insurance firms to mitigate the threat of ransomware. This is problematic because without an open-minded approach from all participants, moving forward to a more sustainable solution could prove challenging. As researchers, we were struck by the incompatibility of some of the statements made by participants. Those working in the industry viewed their role, unsurprisingly, as a positive one working to provide clients with a range of products that vastly widened their potential support mechanisms, a view that is ostensibly true (Woods and Moore, 2020; MacColl et al., 2021). Yet these same support mechanisms were viewed very differently by those participants working in government and law enforcement in particular,

[6] In the case of employers' liability insurance, it is the requirement to protect current and former employees as enshrined in the Employers Liability Act 1969.

however, given that the most effective outcome for an insured may involve facilitating ransom payments and letting the ransomware operatives have their payday.

The truth is likely somewhere in the middle. It is without question that the range of services that cyber insurers offer to an insured that is subject to a cyberattack (ransomware or otherwise) will help all but the biggest firms by providing specialist services that can handle every part of the remediation process. Those services must certainly widen the range of possible actions that insureds under attack can take, and in combination with higher security standards, the argument is that restoration of services should be much quicker and much more possible, with less long-term damage.

However, the focus of those participants in law enforcement and government is that having insurers on standby with deep pockets and a desire to make issues go away fast will necessarily allow for bigger and more frequent ransom payments than otherwise – that is, introducing moral hazard as a result of the easier access to means of ransom payment (Gordon et al., 2003; Bolot and Lelarge, 2009; Bailey, 2014). Those in industry disagreed with this: it is naïve to assume that paying a ransom will immediately return systems to normal, or that any key provided upon payment will even work – and furthermore, it is up to the client whether or not to pay, not the insurer – and yes, it is the insurer's money, but where will the organisation get cyber insurance in the future? But there was also recognition that, in being forced to systematise the response process, it certainly makes the process of paying a ransom – if a client had decided to do so – easier, by ensuring access to negotiators, and even more available access to cryptocurrency when needed. The lack of regulation or professional standards required of negotiation firms, and the slow movement to require reporting from cryptocurrency exchanges were cited by industry participants as issues in running a "clean" service. Recent OFAC statements (Department of the Treasury, 2021) have, at least, started to ensure insurers and reinsurers consider the implications of paying sanctioned entities; it is also the case that, until there is legislative obligation not to pay a ransom, insurers will have to act in ways that are best for their client in the ways that the laws allow (Libatique, 2021).

In all this, though, it is vital to remember the low penetration of cyber insurance amongst organisations in the UK and globally. Whilst the hardening market may serve to raise standards of cyber security practices, this is only ever going to be amongst those that look to be insured. And so, in this respect, the very aspects of cyber insurance that could be said to mitigate the ransomware threat (higher standards, access to professional support before and after breaches) are not accessible to, or required of, the majority of organisations: those that do not seek insurance.

6. Conclusion and future work

This article has explored recent developments in the convergence of escalating ransomware activity and the emerging cyber insurance market to consider whether or not cyber insurance can mitigate the ransomware threat. Drawing on interview and workshop data involving a wide-range of stakeholders in the cyber insurance and cyber security industries, our research has identified that the scale and impacts of contemporary ransomware have presented acute challenges for purchasers and providers of cyber insurance. At the same time, for organisations, ransomware has clarified the potential costs of a cyber breach more tangibly than prior cyber risks. This, in turn, has prompted increased awareness of the utility of cyber insurance, at a time when the market is hardening. With premiums increasing relative to coverage, cyber security prerequisites becoming obligatory, and some industries being labelled as 'uninsurable', cyber insurance – already at relatively low penetration rates – is at risk of becoming more inaccessible at a time when demand and awareness may be at their highest. In this context, the scope for cyber insurance to influence the proliferation of ransomware and its impacts at a societal level – either positively or negatively – is, in practice, limited. It remains far from clear, additionally, if the professionalisation of the remediation process – one typically spearheaded by insurers to help provide seamless assistance to insureds – leads to dubious ethical outcomes, that come down to the basic question of whether it is more efficient to pay the ransom if the liquidity and mechanisms to do so are available? Our participants were split on this issue, however, in an environment wherein there are no 'silver bullet' solutions to preventing ransomware or ensuring resiliency in the event of an incident, cyber insurance is part of a limited basket of viable options that many organisations could employ as part of their cyber resiliency strategy, and one that must not be considered sufficient to stem the threat, without the support of active law enforcement and policy to help lay out what is and is not acceptable practice.

There are various avenues for future research. As means of futureproofing, further research could examine the wider context of the hardening market: was the proliferation of ransomware the sole cause for the hardening market, or did the advent of COVID-19, and the economic impacts it brought, also cause capital to begin to be withheld? This issue could be considered from the UK context but also internationally, particularly in the USA, EU and Asia-Pacific. There is also a need for future research to consider market and government measures that encourage – and support – accessibility to cyber insurance. For instance, in the UK there are initiatives that provide basic cyber insurance coverage to SMEs who acquire the government-backed Cyber Essentials certification. However, little is known about whether, or to what extent, organisations who acquire insurance via this route reduce their exposure to ransomware. There will undoubtedly be similar initiatives across other countries. Another related area worth exploring is how many organisations improve their cyber security standing as a result of awareness – or intention to purchase – cyber insurance, but do not purchase it: could the existence of the product increase cyber security standards?

There is also a need to consider the alternative routes for cyber resiliency for organisations who cannot acquire cyber insurance or cannot get sufficient coverage. Whilst large organisations are likely to be able to self-insure against non-existential cyber incidents, SME and medium-sized organisations are potentially existentially vulnerable to a severe ransomware incident. In cases where organisations who provide critical national infrastructure (CNI) – such as utility firms, local public services or healthcare – cannot acquire sufficient cyber insurance coverage, should the national government be either a tacit (ad-hoc) or overt (institutionalised) actor-of-last-resort?

Separately, this research highlighted that the cyber insurance industry is typically agnostic with respect to the driver of ransomware: the payment of demanded/negotiated ransoms. It was clear that the decision to pay – or not pay – a ransom was to be made by the victim organisation, who would take on board advice from their incident support network – including the importance of ensuring compliance with sanctions checks to ensure repayment, where necessary. Further research would be beneficial into understanding how much visibility the sanctions compliance process gives into the network of ransomware gangs, and how that could be usefully leveraged for law enforcement and policy purposes. Whilst insurers had an indirect preference to keep incident

costs low, this was tempered by the desire to support their clients and maintain client relationships. Interviewees were broadly in agreement that ransom payment was, in any case, an imperfect solution – due to the technical faults of the decryption keys and inability to assess whether stolen data has truly been deleted – but were divided on whether ransom payments should be prohibited. Most interviewees, however, noted that were a ban to be implemented, it should cover *all* ransomware payments, rather than specifically prohibit the coverage of ransomware payments through insurance. There is a necessity for further research on the viability of prohibiting ransomware payments, including assessments of the enforceability of such legislation, as well as potential unintended consequences for the cyber resiliency of victim organisations.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Gareth Mott: Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing. **Sarah Turner:** Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing. **Jason R.C. Nurse:** Conceptualization, Methodology, Investigation, Writing – review & editing, Validation, Supervision, Project administration, Funding acquisition. **Jamie MacColl:** Conceptualization, Methodology, Data curation, Investigation, Validation, Project administration, Funding acquisition. **James Sullivan:** Conceptualization, Project administration, Funding acquisition. **Anna Cartwright:** Conceptualization, Validation. **Edward Cartwright:** Conceptualization, Validation.

Data availability

The authors do not have permission to share data.

Acknowledgements

This research was funded by The Research Institute for Sociotechnical Cyber Security, a collaboration of the UK's Engineering and Physical Sciences Research Council (EPSRC) and the National Cyber Security Centre (NCSC).

Appendix A

Interview Protocol (scoped).

Theme	Questions
Overview	What is your role and industry? How many years of experience do you have in your industry? Have you always worked in cyber? If not, what other sector(s) did you work in before? What types of organisations do you provide services or cover for? Any specific sectors?
The state of the market	What is the state of the cyber insurance market and how has this changed over the last few years? What are the positive and negative impacts of these changes? Has ransomware played a role in the changes in the cyber insurance industry? If so, how? Are all organisations that request cyber insurance coverage currently able to attain it (i.e., to find a company willing to underwrite the policy)?
Cyber insurance and the ransomware threat	What are the roles of the various post-incident services (including your organisation) after a ransomware attack on an insured organisation? How much influence do you have on a policymaker's decision-making during/after a ransomware attack? What sort of post-incident services do cyber insurers provide for ransomware victims? Are these in-house capabilities or third-party capabilities? How is the insurance industry dealing with (the challenges posed by) ransomware? How do insurers assess an organisation's cyber risk? Have underwriting practices changed since ransomware became more of a threat? To underwrite an insurance policy, do insurers now require specific security controls from insureds? If so, which ones? What is the role of cyber insurance in helping organisations the threat of ransomware, particularly its impacts? From an economic perspective, there is an argument that it is often cheaper to pay the ransom than to try to recover from backups. What are your thoughts on this? Are there any other incentives that push victims to pay the ransoms? Are organisations that are insured more likely to pay ransom demands? Under what conditions are insurers willing to pay the ransom? How does an insurance company decide what ransom amount they are willing to pay? Do your policies (or policies that you are aware of) include any kind of warranties or security obligations that need to be fulfilled for a ransomware claim to be paid? For instance, patching vulnerabilities etc. In your opinion, has cyber insurance incentivised more ransomware attacks?

Appendix B

Code book.

Deductive Parent Code	Deductive Sub Code	Theme once analysed Accessibility of cyber insurance	Cyber insurance and cyber minimum security practices	Perceived value of insurance with respect to mitigating ransomware threat
Views of changes in underwriting based on the ransomware threat	Attack surface scans offer a limited picture		✓	✓
	Insureds know more about cyber security or best practices		✓	✓
	Insurers do not have a uniform understanding of best practice		✓	✓
	Insurers don't have mechanism to force insureds to respond to attack surface scans		✓	✓
	Insurers too focused on compliance-based frameworks		✓	✓
	Insurers unwilling to introduce warranties or security obligations		✓	✓
	Low uptake of pre-breach services			✓
	No evidence controls reduce risk		✓	
	Pre-breach services have no impact on cyber security			✓
	Questions too limited or binary		✓	✓
	Too much emphasis on particular controls		✓	✓
	Attack surface scans identifying vulnerabilities or cyber hygiene problems during risk assessments		✓	✓
	Brokers providing roadmap to clients to improve cyber security		✓	
	Brokers using initial assessments to identify and remediate risks	✓	✓	
	Focus is on minimal business interruption			✓
	Insurers driving best practices	✓	✓	✓
	Insurers financially incentivised to reduce risk or improve security of insureds	✓	✓	✓
	Insurers offering consulting risk engineering services to insureds	✓	✓	✓
	Insurers offering regular attack surface scans to insureds	✓	✓	✓
	Insurers providing roadmap to insureds to improve cyber security	✓	✓	✓
	Insurers using warranties or contractual obligations to enforce patching or remediation during period of coverage		✓	✓
	Underwriters offering premium discounts in response to certification to standards	✓	✓	

(*continued on next page*)

Deductive Parent Code	Deductive Sub Code	Theme once analysed Accessibility of cyber insurance	Cyber insurance and cyber minimum security practices	Perceived value of insurance with respect to mitigating ransomware threat
	Underwriters offering premium discounts in response specific security controls	✓	✓	
	Underwriters refusing bad risks	✓	✓	
	Underwriters refusing organisations without minimum security controls	✓	✓	
Impact of insurance on ransomware	Incident response ecosystem has normalised payment of ransoms			✓
	Insurance has normalised payment of ransoms			✓
	Insurance has not normalised payment of ransoms			✓
	Insurance increases sanctions compliance			✓
	Insurer requires a notification to law enforcement before a ransom is paid			✓
	Insurers only want to pay ransoms as a last resort			✓
	Organisations with cyber insurance are more likely to be targeted			✓
	Ransomware groups use cyber insurance policies to increase ransom demands			✓
	Victims with cyber insurance are more likely to pay			✓
	Victims without cyber insurance are more likely to pay			✓
Pricing and terms	Co-insurance on ransomware coverage		✓	
	Coverage is being reduced	✓	✓	
	Excess on ransomware coverage		✓	
	Insurance firms are for-profit		✓	✓
	No changes to ransomware coverage	✓	✓	✓
	Off the shelf pricing for SMEs	✓		
	Premium increases higher for certain sectors or industries	✓		
	Premiums are increasing	✓		
	Premiums are too expensive for businesses	✓		
	Views on what happens to premiums as market softens		✓	
	Price increase not big issue for business	✓		
	Sub-limits on ransomware coverage		✓	

(*continued on next page*)

Deductive Parent Code	Deductive Sub Code	Theme once analysed Accessibility of cyber insurance	Cyber insurance and cyber minimum security practices	Perceived value of insurance with respect to mitigating ransomware threat
Purchasing decisions	Board wants cyber insurance			✓
	Essential purchase now			✓
	Media reporting			✓
	Need for post-breach services			✓
	Regulatory requirement			✓
	Risk transfer			✓
	Understanding of risk			✓
	Already have IR retainer			✓
	Believe cyber insurance is ineffective		✓	✓
	Coverage is too limited		✓	✓
	Do not believe insurers understand cyber risk		✓	✓
	Do not trust insurance			✓
	Faith in existing cyber security or risk management practices		✓	✓
	Not mandatory			✓
	See cyber insurance as a luxury			✓
	Self-insure			✓
	Too expensive	✓		
Purpose of cyber insurance	Access to services			✓
	Business continuity			✓
	Views on data breach being a concern of insureds			✓
	Financial Coverage			✓
	Protection against ransomware			✓
	Risk transfer			✓
Security Controls	Advice on implementation of controls provided by broker		✓	
	Views on certification to security standards		✓	
	Controls based on claims data		✓	✓
	Controls based on industry best practices or security standard		✓	✓
	Controls required depend on size of business or sector		✓	✓
	EDR solution required		✓	
	Focus is on minimal business interruption			✓
	IAM controls required		✓	
	MFA on all accounts required		✓	
	MFA on remote access or administrator accounts required		✓	
	Network segmentation required		✓	
	Regular patching cadence required		✓	
	Remote access controls required		✓	
	Roadmap for introduction of controls after policy is taken out		✓	
	Segmented, offline backups required		✓	
	Training required		✓	

(*continued on next page*)

Deductive Parent Code	Deductive Sub Code	Theme once analysed Accessibility of cyber insurance	Cyber insurance and cyber minimum security practices	Perceived value of insurance with respect to mitigating ransomware threat
State of the Market	Brokers won't take bad risks to market	✓	✓	
	Businesses not taking security footing seriously	✓	✓	✓
	Capacity is decreasing	✓		
	Cyber is a new class			✓
	Data breaches difficult to price	✓		✓
	Demand is increasing	✓		✓
	Everyone can still find coverage somewhere	✓		
	Insurers leaving the market	✓		✓
	Insurers removing bad risks from their books	✓		✓
	Minimum security requirements preventing organisations from getting coverage	✓	✓	
	Not enough expertise in assessing risk in the market		✓	✓
	Not everyone can get coverage	✓		
	Signs of market failure	✓		✓
	Views on SMEs as a business risk	✓	✓	✓
	Some sectors or industries can't get coverage	✓		
	Specific insurers reducing capacity	✓		
Victim decision-making during a ransomware incident	Breach counsel is most influential actor on victim decision-making			✓
	GDPR makes victims more likely to pay			✓
	Insurance has no impact on decision to pay a ransom			✓
	Insurance structure influencing behaviour			✓
	Insurers actively influence victim decision-making			✓
	Insurer's and victim's interests and priorities are aligned			✓
	Insurer's and victim's interests and priorities are not aligned			✓
	Insurers have no impact on victim decision-making			✓
	Insurers passively influence victim decision-making			✓
	Insurer's priority is to reduce costs			✓
	Victims ignore advice on ransom payments			✓
	Victims make their own decisions			✓
	Victims that suffer double extortion are more likely to pay			✓
	Victims with cyber insurance have more options			✓
	Victims with insurance are more likely to pay ransoms			✓
	Victims without insurance are more likely to pay ransoms			✓

Appendix C

Workshop Provocations.

Provocations
With premiums rising and coverage falling, has the value proposition of cyber insurance changed for businesses?
In your experience, are there any sectors/types of organisations struggling to find coverage? If so, how can/should government intervene?
Are the types of security controls now requested by underwriters proportional to the risk? Are they being applied across the board or is the SME market still soft? Do security practitioners believe these are the right controls to mitigate current cyber threats?
Are the security controls now being requested by underwriters realistic for organisations to implement?
What constitutes minimum due diligence for sanctions compliance for insurers and victims?
Interviewees from the insurance industry often say they reimburse ransoms as a 'last resort' – what constitutes a 'last resort' in your experience?
Interviewees from the insurance industry often say that insurance gives 'other options' to victims. What exactly are those other options in practice?
How can insurance incentivise victims not to pay the ransom? Does this require government intervention?

References

Abdul Hamid, N.H.A., Nor, M., Hussain, F.M., Raju, R., Naseer, H., Ahmad, A, 2022. Barriers and enablers to adoption of cyber insurance in developing countries: an exploratory study of Malaysian organizations. Comput. Secur. 122. doi:10.1016/j.cose.2022.102893, Available at.

Abraham, K.S., Schwarcz, D, 2021. Courting Disaster: the Underappreciated Risk of a Cyber-Insurance Catastrophe. Connecticut Insurance Law J.. [Preprint]Available at http://www.ssrn.com/link/U-Virginia-LEC.htmlPublicLawandLegalTheory:http://www.ssrn.com/link/U-Virginia-PUB.htmlElectroniccopyavailableat:https://ssrn.com/abstract=3792882 .

Agrafiotis, I., Nurse, J.R.C., Goldsmith, M., Creese, S., Upton, D, 2018. A taxonomy of cyber-harms: defining the impacts of cyber-attacks and understanding how they propagate. J. Cybersecur. doi:10.1093/cybsec/tyy006, Available at.

Allianz, 2022. Allianz Risk Barometer Available at https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html .

Aon, 2022. *Market impact, Aon* Available at https://publications.aon.com/eo-and-cyber-market-review/market-impact .

Bailey, L.M.D., 2014. Mitigating Moral Hazard in Cyber-Risk Insurance. J. Law Cyber Warfare 3 (1), 1–42. http://www.jstor.org/stable/26432557.

Bloomberg, 2022. Corvus Insurance Reports Ransomware Attacks Are Down from Recent Peaks As Costs and Frequency of Claims Trend Downward. Bloomberg Available at https://www.bloomberg.com/press-releases/2022-04-13/corvus-insurance-reports-ransomware-attacks-are-down-from-recent-peaks-as-costs-and-frequency-of-claims-trend-downward .

Bolot, J., Lelarge, M., 2009. Cyber Insurance as an Incentivefor Internet Security. In: Johnson, M.E. (Ed.), Managing Information Risk and the Economics of Security. Springer, Boston, MA doi:10.1007/978-0-387-09762-6_13.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3 (2), 77–101. doi:10.1191/1478088706qp063oa, Available at.

Brumfield, C., 2022. White House ransomware Summit Highlights Need For Borderless Solutions. CSO Online Available at https://www.csoonline.com/article/3678948/white-house-ransomware-summit-highlights-need-for-borderless-solutions.html .

Bryman, A., 2016. Social Research Methods, 5th edn. Oxford University Press, London.

Buchanan, B., 2016. The life cycles of cyber threats. Survival (Lond.) 58 (1), 39–58. doi:10.1080/00396338.2016.1142093, Available at.

Buckley, J., 2021. The industrialisation of cyber extortion. Comput. Fraud Secur. (12) 6–10 2021.

Catota, F.E., Granger Morgan, M., Sicker, D.C., 2019. Cybersecurity education in a developing nation: the Ecuadorian environment. J. Cybersecur. 5 (1). doi:10.1093/cybsec/tyz001, Available at.

Cho, E., 2021. Why the hardening cyber market benefits all. Munich Re. Available at https://www.munichre.com/topics-online/en/digitalisation/cyber/hardening-cyber-market.html . Accessed: 9 August 2022.

Cimpanu, C., 2021. Swiss cloud becomes the latest web hosting provider to suffer a ransomware attack. Record. Available at https://therecord.media/swiss-cloud-becomes-the-latest-web-hosting-provider-to-suffer-a-ransomware-attack . (Accessed: 29 July 2021).

Check Point Research (2022) *Behind the Curtains of the Ransomware Economy - the victims and the Cybercriminals*. Available at: https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/ (Accessed: 9 August 2022).

CISA (2022) *CISA,FBI, NSA and International Partners Issue Advisory on Ransomware Trends from 2021 - CISA*. Available at: https://www.cisa.gov/news/2022/02/09/cisa-fbi-nsa-and-international-partners-issue-advisory-ransomware-trends-2021 (Accessed: 22 February 2022).

Cluley, G. (2021) *Ransomware gang says it targets firms who have cyber insurance, Graham Cluley*. Available at: https://grahamcluley.com/ransomware-gang-says-it-targets-firms-with-cyber-insurance/ (Accessed: 4 November 2022).

CNBC, 2021. Ransomware attack may have impacted thousands of small businesses. CNBC. Available at https://www.cnbc.com/2021/07/03/ransomware-attack-may-have-impacted-thousands-of-small-businesses.html . Accessed: 15 August 2022.

Connolly, L.Y., Wall, D.S, 2019. The rise of crypto-ransomware in a changing cybercrime landscape: taxonomising countermeasures. Comput. Secur. 87. doi:10.1016/j.cose.2019.101568, Available at.

Connolly, L.Y., Wall, D., Lang, M., Oddson, B., 2020. An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. J. Cybersecur. 6 (1). doi:10.1093/CYBSEC/TYAA023, Available at.

Coveware (2020) *Ransomware amounts rise 3× in Q2 as Ryuk and Sodinokibi spread*. Available at: https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread (Accessed: 2 August 2021).

Coveware (2021) *Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority*. Available at: https://www.coveware.com/blog/2021/7/23/q2-ransom-payment-amounts-decline-as-ransomware-becomes-a-national-security-priority (Accessed: 2 August 2021).

Cremer, F., Sheehan, B., Fortmann, M., Kia, A., Mullins, M., Murphy, F., Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap. Risk Insur. Issues Pract. 47 (3), 698–736. doi:10.1057/s41288-022-00266-6, Available at.

Curtis, H., 2022. Analysis: what's holding back the SME market from taking up cyber insurance? Insurance Post. Available at https://www.postonline.co.uk/commercial/7950111/analysis-whats-holding-back-the-sme-market-from-taking-up-cyber-insurance . (Accessed: 15 August 2022).

Cowbell, 2020. *Cowbell Cyber finds small-to-medium-sized enterprises (SMEs) more likely to adopt cyber insurance, Cowbell*. Available at: https://cowbell.insure/news-events/pr/cowbell-cyber-finds-small-to-medium-sized-enterprises-smes-more-likely-to-adopt-cyber-insurance/ (Accessed: 15 August 2022).

Davidson, R., 2021. The fight against malware as a service. Netw. Secur. (8) 7–11. doi:10.1016/S1353-4858(21)00088-X, 2021Available at.

Databarracks, 2021. *Over half of businesses now have a policy on whether to pay out on ransomware attacks, says Databarracks research*. Available at: https://www.databarracks.com/news/over-half-of-businesses-now-have-a-policy-on-whether-to-pay-out-on-ransomware-attacks-says-databarracks-research (Accessed: 2 August 2021).

Department for Digital, Culture, Media and Sport (2022) *Cyber Breaches Survey 2022*. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022 (Accessed: 13 January 2023).

Department for International Trade, 2021. *Department For International Trade (DIT) Small and Medium Enterprises (SME) Action Plan*. Available at: https://www.gov.uk/government/publications/dit-small-and-medium-enterprises-sme-action-plan/department-for-international-trade-dit-small-and-medium-enterprises-sme-action-plan. (Accessed: 10 August 2022).

Department of the Treasury, 2021. *Updated advisory on potential sanctions risks for facilitating ransomware payments, Department of the Treasury*. Available at: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (Accessed: 8 November 2022).

Dignan, L., 2021. *Cyber insurance premiums, take-up rates surge. says GAO, Zdnet*. Available at: https://www.zdnet.com/article/cyber-insurance-premiums-take-up-rates-surge-says-gao/ (Accessed: 9 August 2022).

DuChene, C., 2022. *It's high time we address the cyber insurance talent gap. What will it take to secure the future?, Risk Insurance*. Available at: https://riskandinsurance.com/its-high-time-we-address-the-cyber-insurance-talent-gap-what-will-it-take-to-secure-the-future/ (Accessed: 13 January 2023).

Dudley, R., 2019. The extortion economy: how insurance companies are fueling a rise in ransomware attacks. ProPublica. Available at https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks . (Accessed: 4 November 2022).

Edmundson, P., 2021. Tips from top brokers: how to play offense in a cyber hard market. Corvus. Available at https://www.corvusinsurance.com/blog/tips-from-top-brokers-how-to-play-offense-in-a-cyber-hard-market . Accessed: 9 August 2022.
Eling, M., Jung, K., Shim, J., 2022. Unraveling heterogeneity in cyber risks using quantile regressions. Insurance: Math. Econ. 104, 222–242. doi:10.1016/j.insmatheco.2022.03.001, Available at.
Evans, S., 2020. *Why cyber re/insurance needs ILS – Q&A with Tom Johansmeyer, PCS, Artemis*. Available at: https://www.artemis.bm/news/why-cyber-re-insurance-needs-ils-qa-with-tom-johansmeyer-pcs/ (Accessed: 11 November 2022).
Franke, U., 2017. The cyber insurance market in Sweden. Comput Secur 68, 130–144. doi:10.1016/j.cose.2017.04.010, Available at.
Gordon, L., Loeb, M., Sohail, T., 2003. A framework for using insurance for cyber-risk management. Commun. ACM 46 (3), 81–85.
Hadan, H., Serrano, N., Camp, L.J., 2021. A holistic analysis of web-based public key infrastructure failures: comparing experts' perceptions and real-world incidents. J. Cybersecur. 7 (1). doi:10.1093/cybsec/tyab025, Available at.
Harvey, J.T., 2022. The need for national cyber insurance - a lesson to be relearned. *Cyber Defense* Rev. 7 (1), 207–216.
Holmes, A., 2022. Companies are ditching cybersecurity insurance as premiums rise, coverage shrinks. The Information. Available at https://www.theinformation.com/articles/companies-are-ditching-cybersecurity-insurance-as-premiums-rise-coverage-shrinks . Accessed: 8 November 2022.
HSB, 2021. *HSB acquires Zeguro's cybersecurity digital platform for small business, Munich Re*. Available at: https://www.munichre.com/hsb/en/press-and-publications/press-releases/2021/2021-10-21-hsb-acquires-zeguro-cybersecurity-digital-platform.html (Accessed: 8 November 2022).
ISO (no date) *ISO/IEC 27001 and related standards: information security management, ISO*. Available at: https://www.iso.org/isoiec-27001-information-security.html (Accessed: 8 November 2022).
Jenkins, A. and Ventham, E., 2022. *Is cyber insurance exacerbating the ransomware crisis?, InfoSecurity*. Available at: https://www.infosecurity-magazine.com/magazine-features/cyber-insurance-ransomware-crisis/ (Accessed: 4 November 2022).
Jimenez-Sanchez, K., 2022. *Growth potential for cyber insurance market could be improved: cyberCube's Bole, Reinsurance News*. Available at https://www.reinsurancene.ws/growth-potential-for-cyber-insurance-market-could-be-improved-cybercubes-bole/ (Accessed: 13 January 2023).
Kenneally, J., Goody, K., Shilko, J., 2020. Navigating the Maze: tactics, techniques and procedures associated with Maze ransomware incidents. FireEye. Available at https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html . (Accessed: 31 August 2021).
Khodjibaev, A., Korzhevin, D., McKay, K., 2021. *Interview With a LockBit ransomware Operator*. New York.Available at. https://blog.talosintelligence.com/interview-with-lockbit-ransomware/.
Knutson, T., 2021. Small businesses bearing brunt of ransomware attacks, Senate told. Forbes. Available at https://www.forbes.com/sites/tedknutson/2021/07/27/small-businesses-bearing-brunt-of-ransomware-attacks-senate-told/?sh=3feddaf09556. (Accessed: 15 August 2022).
Kudale, J., 2021. The future of cybersecurity insurance: policies that follow the risk. Forbes. Available at https://www.forbes.com/sites/theyec/2021/08/17/the-future-of-cybersecurity-insurance-policies-that-follow-the-risk/?sh=1c1a19055f5b. (Accessed: 9 August 2022).
Lallie, H.S., Shepherd, L.A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., Bellekens, X., 2020. Cyber Security in the Age of COVID-19: a Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic. Comput. Secur. doi:10.1016/j.cose.2021.102248, Available at.
Lawton, S. (2022a) *Experts offer advice on cyber insurance trends, qualifying for coverage, Sophos*. Available at: https://news.sophos.com/en-us/2022/03/25/experts-offer-advice-on-cyber-insurance-trends-qualifying-for-coverage/ (Accessed: 9 August 2022).
Lawton, S. (2022b) *How to qualify for cyber insurance, Sophos News*. Available at: https://news.sophos.com/en-us/2022/03/16/how-to-qualify-for-cyber-insurance/ (Accessed: 9 August 2022).
Lerman, R., de Vynck, G., 2021. Ransomware claims are roiling an entire segment of the insurance industry. Washington Post. Available at https://www.washingtonpost.com/technology/2021/06/17/ransomware-axa-insurance-attacks . (Accessed: 2 August 2021).
Li, Y., Mamon, R., 2023. Modelling health-data breaches with application to cyber insurance. Comput. Secur. 124, 102963. doi:10.1016/j.cose.2022.102963, Available at.
Libatique, R., 2021. Insurance giants call on government to outlaw ransomware payments. Insurance Bus.. Available at https://www.insurancebusinessmag.com/au/news/cyber/insurance-giants-call-on-government-to-outlaw-ransomware-payments-259136.aspx . (Accessed: 9 August 2022).
Logan, M., Mendoza, E., Maglaque, R., Tamana, N., 2021. The state of ransomware. Trend Micro. Available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-state-of-ransomware-2020-s-catch-22 . (Accessed: 28 July 2021).
Logue, K.D. and Shniderman, A.B., 2021. *The case for banning (and mandating) ransomware insurance the case for banning (and mandating) ransomware* Available at: https://ssrn.com/abstract=3907373.
Lucas, P., 2018. There is more to terrorism insurance than just Pool Re. Insurance Bus.. Available at https://www.insurancebusinessmag.com/uk/news/kidnap-ransom-terrorism/there-is-more-to-terrorism-insurance-than-just-pool-re-117634.aspx . (Accessed: 15 August 2022).
MacColl, J., Nurse, J.R.C. and Sullivan, J., 2021. *Occasional paper cyber insurance and the cyber security challenge*. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge. (Accessed: 9 February 2022).
Markopoulou, D., 2021. Cyber-insurance in EU policy-making: regulatory options, the market's challenges and the US example. Computer Law Secur. Rev. 43, 105627. doi:10.1016/j.clsr.2021.105627, Available at.
Marzouk, Z., 2021. French insurer AXA suffers ransomware attack in Asia. ITPro. Available at https://www.itpro.com/security/ransomware/359565/french-insurer-axa-suffers-cyber-attack-in-asia . Accessed: 9 August 2022.
Mehrotra, K., Turton, W., 2021. CNA Financial paid $40 million in ransom after March cyberattack. Bloomberg. Available at https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack#xj4y7vzkg . (Accessed: 9 August 2022).
Millman, R., 2021. *Average ransomware costs have more than doubled in 2021, IT Pro*. Available at: https://www.itpro.co.uk/security/ransomware/359364/cost-of-ransomware-doubles-in-a-year (Accessed:7 February 2022).
Muncaster, P., 2022. *Swiss Re: cyber-insurance industry must reform, InfoSecurity*. Available at: https://www.infosecurity-magazine.com/news/swiss-re-cyberinsurance-industry/ (Accessed: 13 January 2023).
NCSC, 2021. Update to the cyber essentials technical controls. NCSC. Available at https://www.ncsc.gov.uk/information/update-to-the-cyber-essentials-technical-controls . (Accessed: 15 August 2022).
National Cyber Security Centre, 2018. *Supply chain attack examples - NCSC.GOV.UK, NCSC*. Available at: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples (Accessed: 31 August 2021).
NIST (2018) Cybersecurity framework, NIST. Available at: https://www.nist.gov/cyberframework (Accessed: 8 November 2022).
Nurse, J.R.C., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S., 2020. The data that drives cyber insurance: A study into the underwriting and claims processes. In: International conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, pp. 1–8. doi:10.1109/CyberSA49311.2020.9139703.
Osborne, C., 2021. Updated Kaseya ransomware attack FAQ: what we know now. Zdnet. Available at https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now . (Accessed: 19 August 2021).
Pain, D., Noordhoek, D, 2022. Ransomware: an insurance market perspective. Geneva Assoc.. Available at https://www.genevaassociation.org/sites/default/files/ransomware_report_online.pdf . (Accessed 13 January 2023).
Palmer, D., 2022. *Ransomware gangs are changing their tactics. That could prove very expensive for some victims*. Available at: https://www.zdnet.com/article/ransomware-gangs-are-changing-their-tactics-that-could-prove-very-expensive-for-some-victims/ (Accessed: 9 August 2022).
Rafferty, I., 2021. Cyber insurance industry predicted to exceed $20bn GWP by 2025 – GlobalData. Insurance Times. Available at https://www.insurancetimes.co.uk/news/cyber-insurance-industry-predicted-to-exceed-20bn-gwp-by-2025-globaldata/1438074.article . (Accessed: 3 August 2021).
Reshmi, T.R., 2021. Information security breaches due to ransomware attacks - a systematic literature review. Int. J. Inf. Manage. 1 (2), 100013. doi:10.1016/j.jjimei.2021.100013, Available at.
Rivero, N., 2021. *Ransomware hacks are pushing cyber insurance premiums to record levels, Quartz*. Available at: https://qz.com/2036127/ransomware-hacks-are-driving-up-premiums-for-cyber-insurance/ (Accessed: 7 February 2022).
Romanosky, S., Ablon, L., Kuehn, A., Jones, T., 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. 5 (1). doi:10.1093/cybsec/tyz002, Available at.
Ruel, C., 2021. BrokerFest 2021: sustained period of cyber market hardening must be fully understood. Insurance Times. Available at https://www.insurancetimes.co.uk/news/brokerfest-2021-sustained-period-of-cyber-market-hardening-must-be-fully-understood/1439254.article . (Accessed: 15 August 2022).
Ryan, T., 2016. *Cyber Liability insurance: As the Market Heats up, is It Time to Cool Off in a Pool?*, Milliman.
Sales, N., 2013. Regulating Cyber-security. Nw. U. L. Rev. 107, 1503. Available at https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss4/1 . (Accessed: 10 January 2023).
Schneier, B., 2001. Insurance and the computer industry. Commun. ACM 44 (3), 114–115. doi:10.1145/365181.365229, March 2001.

Sheehan, M., 2022. *Hardening cyber market shows no signs of slowing: berenberg, Reinsurance News*. Available at: https://www.reinsurancene.ws/hardening-cyber-market-shows-no-signs-of-slowing-berenberg/ (Accessed: 15 August 2022).
Smilyanets, D., 2021. 'I scrounged through the trash heaps … now I'm a millionaire:' an interview with REvil's unknown. Record. Available at https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown . (Accessed: 7 February 2022).
Smith, I., 2021. Cyber insurers recoil as ransomware attacks 'skyrocket. Financ. Times. Available at https://www.ft.com/content/4f91c4e7-973b-4c1a-91c2-7742c3aa9922 . (Accessed: 7 February 2022).
Uuganbayar, G., Yautsiukhin, A., Martinelli, F., Massacci, F., 2021. Optimisation of cyber insurance coverage with selection of cost effective security controls. Comput. Secur. 101. doi:10.1016/j.cose.2020.102121, Available at.
White House, 2022. *Fact sheet: the second international counter ransomware initiative summit*. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/ (Accessed: 4 November 2022).
US Small Business Administration Office of Advocacy, 2020. *Frequently asked questions*. Available at: https://cdn.advocacy.sba.gov/wp-content/uploads/2020/11/05122043/Small-Business-FAQ-2020.pdf (Accessed: 10 August 2022).
Sophos, 2022. *The state of ransomware 2022*. Available at: https://assets.sophos.com/X24WTUEQ/at/4zpw59pnkpxxnhfhgj9bxgj9/sophos-state-of-ransomware-2022-wp.pdf (Accessed: 1 January 2023).
NIST (no date) *Cybersecurity framework, NIST*. Available at: https://www.nist.gov/cyberframework (Accessed: 8 November 2022).
Wolff, J., Lehr, W., 2018. Roles for Policy-Makers in Emerging Cyber Insurance Industry Partnerships. TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141409.
Woods, D., Bohme, R., Wolff, J., Schwarcz, D, 2023. Lessons lost: incident response in the age of cyber insurance and breach attorneys. In: *Proceedings of the 32nd USENIX Security Symposium*. Anaheim: The 32nd USENIX Security Symposium. Available at.
Woods, D., Simpson, A., 2017. Policy measures and cyber insurance: a framework. J. Cyber Policy 2 (2), 209–226. doi:10.1080/23738871.2017.1360927, Available at.
Woods, D.W., Moore, T., 2020. Does insurance have a future in governing cybersecurity? IEEE Secur. Priv. 18 (1), 21–27. doi:10.1109/MSEC.2019.2935702, Available at.
Zank, A., 2022. No commonality on cyber applications any time soon: advisen panel. Advisen. Available at https://www.advisen.com/tools/fpnproc/fpns/articles_new_35/P/423390254.html?rid=423390254&list_id=35. (Accessed: 9 August 2022).

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

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

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

Jamie MacColl is a Research Fellow in cyber threats and cyber security at the Royal United Services Institute (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. Current research projects focus on cyber insurance and cyber risks related to the Globalisation of Technology. Prior to joining RUSI, he was a researcher at Orpheus Cyber where he provided strategic and operational intelligence analysis on the cyber threat landscape. Jamie holds an MPhil in International Relations and Politics from the University of Cambridge, where his research focused on UK policy towards Russia since the end of the Cold War. He also holds a BA in War Studies from King's College London, where he was awarded the Sir Michael Howard Excellence Award in 2016 and 2018.

James Sullivan is the Director of Cyber Research at RUSI. He founded and has grown a research group at RUSI that considers a number of themes including: the role of national cyber strategies, the cyber threat landscape, cyber security and risk management, offensive cyber, cyber statecraft and diplomacy, and ransomware. James joined RUSI from Deloitte's Cyber Risk team where he provided analysis on the cyber threat landscape and advised on defensive measures and risk management strategies. Prior to this, James worked at the National Crime Agency as an Intelligence Analyst specialising in cybercrime threats. James has contributed to a variety of publications and media outlets such as the FT, BBC and CNN and has provided private briefings on aspects of the cyber threat to high-level fora such as the G7.

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

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