Challenge 6: Incentivising Negative Behaviours There is a possibility that cyber insurance may be actively encouraging negative behaviours for both businesses and cybercriminals. In terms of businesses, the empirical evidence collected as part of this paper highlights that the moral hazard phenomenon is not occurring at scale with cyber insurance. However, cyber insurers may be unintentionally facilitating the behaviour of cybercriminals by contributing to the growth of targeted ransomware operations. The Moral Hazard Some theoretical studies have argued that organisations are less likely to invest in risk prevention if they think that their cyber insurance policy will resolve (and/or cover the cost of) an incident anyway. This phenomenon is known as the 'moral hazard'.208 For boards or senior management not inclined to defer to cyber security practitioners, cyber insurance could be viewed as a replacement for more costly cyber security measures.209 If widespread, this could outweigh the potential positive benefits of cyber insurance by actively encouraging insecure practices and behaviours. It could also drive up insurance premiums, placing an increased financial burden on companies who do invest in cyber security and practice secure behaviours.210 However, research for this paper did not find strong empirical evidence indicating that the moral hazard is a significant issue for cyber insurance. While some insurers did suggest they had seen instances of businesses – particularly SMEs – treat cyber insurance as a substitute for increasing investment in cyber security,211 most interviewees suggested that while the moral hazard could potentially occur, it is not often seen. This chimes with findings from DCMS's 'Cyber Security Breaches Survey 2019', which suggested that organisations consider cyber insurance as complementary to – rather than a substitute for – other forms of cyber risk management.212 This is primarily because cyber insurance policies do not cover all the potential impacts of cyber risk. For instance, financial coverage from a cyber insurance policy will not cover long-term reputational costs that can result from a data breach or ransomware attack, particularly if customer data is affected.213 As one financial services provider stressed, 'there's no amount of cyber insurance pay-out that can remedy a severe loss of reputation'.214 While this argument rests to some extent on the assumption that policyholders understand cyber risk, purchasers of cyber insurance do appear to have a greater understanding of the economic impacts of cyber incidents.215 Moreover, the moral hazard issue may be attenuated by some of the scepticism around cyber insurance – specifically, that financial limits are too low to cover the costs of an incident and that organisations are not certain their policy will pay out.216 In sum, the moral hazard – as theoretically conceived – is not a significant .challenge for the cyber insurance sector, at least no more so than it is for other insurance lines