Written evidence submitted by Dr Gareth Mott, Sarah Turner and Dr Jason R.C. Nurse

This submission was prepared by: Dr Gareth Mott, Sarah Turner and Dr Jason R.C. Nurse from the Institute of Cyber Security for Society (iCSS), University of Kent

We are writing as active academic researchers in the field of socio-technical cyber security, internet governance, cyber crime and cyber resilience (at organisational and national levels). We are delighted to be given this opportunity to respond to the call for evidence relating to the novel risk of ransomware.

In our response, we draw upon inferences and findings from two particular strands of original research that we have undertaken, funded by The Research Institute for Sociotechnical Cyber Security (RISCS) and The National Cyber Security Centre (NCSC), and in collaboration with The Royal United Services Institute (RUSI).

The first strand of research, completed in 2021-22, relates to the role that cyber insurance may play in mitigating ransomware. The second strand of research, running from 2022-23, explores the harms of ransomware; including financial and non-financial harms, and the experience of victims of attacks. For the former project, we conducted original interviews with 65 industry stakeholders, particularly from the cyber security and cyber insurance industries. Our interviews for the latter project are currently ongoing.

Our written response focuses primarily on the following area:

> *The UK victim experience, including sources of support for prevention, detection and recovery, public-private partnerships, the role of the media, access to and availability of insurance cover, and regulatory requirements placed on ransomware victims.*

1. Ransomware is part of a portfolio of risks that contemporary organisations face today. In terms of cyber-risks specifically, ransomware may be the most prescient threat to organisations. The proliferation of ransomware has been exacerbated by the growth of the ransomware ecosystem, including threat-actor professionalisation, the rise of ransomware 'affiliate' programs, and 'ransomware as a service'. **Interviewees generally intimated that the scale of the threat to UK organisations is likely to get worse before it gets better; particularly given the ongoing jurisdictional challenges of intervening against threat actors based in – relatively – permissive nation-states**.

2. As ransomware operators have shifted from relatively indiscriminate targeting to 'big game hunting' and/or opportunism, all organisations from micro-SME level to multinational firms are potentially at risk. The threat actors continue to diversify their approach to monetising cyber security and data vulnerabilities. For instance, UK organisations have, broadly speaking, improved their critical cyber resilience measures so that – were there systems to be maliciously encrypted – they could resume operational functions as soon as possible by drawing on secure, offline backups. **In the face of improvements to organisational cyber resilience, the ransomware threat actors have not only diversified their ecosystem, but have also adopted additional methods of extortion, including 'double', 'triple' or even**

'quadruple' extortion. In a typical extortion attack, the ransomware operators may exfiltrate an organisation's data prior to malicious encryption; threatening to distribute or sell the data if a demanded ransom is not paid.

3. **Amidst the escalating proliferation of ransomware, cyber insurance has been viewed as one potential solution for organisational cyber resilience**. Typically sold as an add-on or stand-alone product, cyber insurance can offer organisations financial coverage in the event of a cyber incident (Nurse et al., 2020). In the case of a typical ransomware attack, for instance, an organisation with sufficient cyber insurance coverage could draw upon the policy to variously cover: the cost of operational downtime; incident response; legal support; PR support; ransom negotiation and payment. In the latter case, the organisation pays the ransom themselves, and would be subsequently reimbursed by the insurer.

4. A variety of stakeholders from the cyber insurance ecosystem highlighted that **the prominent growth of the ransomware threat has prompted organisations to increasingly consider cyber insurance as a viable means of offsetting contemporary cyber risk(s)**. On the other hand, the proliferation of ransomware has presented significant challenges for cyber insurers (MacColl, Nurse and Sullivan, 2021). **Whilst cyber insurance, despite its low-penetration rates, was typically considered a profitable insurance line, ransomware disrupted this**. It was identified that in recent years, some cyber insurers were making losses on their cyber insurance products because of the scale of claims prompted by ransomware. This, in turn, along with other factors arguably prompted a hardening of the market.

5. A particular symptom of this hardening has been a reduction in coverage relative to (increasing) premiums. Additionally, for clients above the micro-SME market, insurers have become much more proactive in assessing the cyber security efficacy of prospective insureds. A prospective insured might now be expected to demonstrate that they have secure offline backups, regular patching cadence, MFA, port controls and more. Failure to demonstrate sufficient cyber security controls may prompt a refusal of coverage, reduced coverage, or limited coverage until necessary controls are in place. **Consumers of cyber insurance reported that they increasingly found the renewal process to be a 'dragons den' experience.** Driven by the escalating costs of premiums and the reduction in coverage, some consumers of cyber insurance noted that their organisations were increasingly reassessing whether cyber insurance was a viable investment.

6. **Of particular note are the growing prominence of possibly 'uninsurable' sectors often influenced by the looming threat of ransomware (and perceived increased susceptibility of some sectors)**. We noted that prospective insureds in particular sectors are increasingly finding that even if they have relatively high-levels of socio-technical cyber security in place, their 'sector' status may prohibit them from accessing viable cyber insurance coverage because of insurers' assessments of the overall risks of their sector. These sectors are notable for either having historically

under-funded cyber security, possessing highly valuable data, and/or being acutely at risk of operational disruption time.

7. **The convergence of ransomware and cyber insurance thus presents a dilemma. Ransomware – more than any prior cyber risk – has clarified the financial risks of cyber threat(s), generating a stronger rationale for organisations to A) invest in cyber security practices to deter incidents and improve resilience and B) invest in cyber insurance as a means of offsetting possible financial losses resulting from a future incident**. However, as insurers reassess their risk exposure to ransomware and apply greater scrutiny to their portfolios, **our research identified that cyber insurance has become increasingly inaccessible**.

8. For some organisations with significant financial reserves, cyber insurance may be purchased as 'an option'. Typically, large organisations would have their own incident response firms on retainer and would eschew an insurer's promoted panel(s). For such organisations, cyber insurance may be an additional safety net, or something that is purchased to ease supply chain contracts, with the existence of cyber insurance being taken as a de facto 'badge' of sufficient cyber resiliency and/or sufficient cyber security controls. **For other organisations with limited financial reserves, cyber insurance may be the *only* viable means of offsetting the financial risks of a potential ransomware breach**. Where such organisations are denied sufficient coverage or cannot afford sufficient coverage, in extremis, they may face an existential crisis in the event of a severe ransomware incident.

9. Ergo, cyber insurance has a capacity to alleviate the harms (Agrafiotis et al., 2018) of ransomware for contemporary organisations. This capacity to alleviate, however, is potentially tempered by the hardening of the market. **Separately, our research also considered whether cyber insurance could be exacerbating the proliferation of ransomware; particularly by offering potential reimbursement of demanded/negotiated ransoms**. The basic hypothetical logic would be that, where an organisation might otherwise be unable to pay a ransom (i.e., cannot afford it) without cyber insurance coverage, cyber insurance coverage may mean that a payment is made to a criminal organisation. Similarly, another basic hypothetical logic might be that some organisational decision-makers may 'offset' the moral quandary of the decision to pay/not pay, if the pool of money ultimately comes from a third party.

10. **Our research suggests that this would be an over-simplification, and would not be representative of the experiences of cyber insurance consumers, cyber insurance stakeholders, and members of the incident response ecosystem. Uniformly, it was highlighted that insurers are kept abreast of decision making, but are not themselves involved in the decision to pay or not pay a ransom. That decision, ultimately, is made by the client organisation**. The client organisation would likely draw upon the advice of third party support, but the client would be the ultimate decision-maker. In this sense, a cyber insurance provider may arguably be agnostic towards ransom payment; at least in some aspects.

11. **The main caveat to this is that there may be instances where payment of a ransom would breach sanctions-regime compliance**. An insurer would advise against and refuse to reimburse a paid ransom if it is found to have breached sanctions compliance. As such, insurers and the incident response ecosystem stakeholders facilitate sanctions checks. Outside of sanctions breaches, the insurer's primary objective is to support their client as best as possible. **Generally, it was highlighted that, on balance, the support network and financial cushion offered by cyber insurance – in additional to demands about cyber security controls – meant that insured clients were less likely to have to pay a demanded ransom versus non-insureds**.

12. **Interviewees were split on the debate about banning ransoms; slightly favouring *not* banning ransom payments. However, there was near-uniform consensus that, were a ban to be implemented, it should cover *all* payments of ransoms, rather than specifically cover insurance reimbursement of ransom payments**. Additionally, there was widespread warmth towards data-sharing between insurers and government; however, this data-sharing channel would likely need to be dual-directional, with government sources sharing meaningful threat intelligence to insurers in return for their data about incidents, which, in essence, forms part of their valuable intellectual property.

We have endeavoured to keep this written response brief and direct, covering a range of critical contemporary developments with respect to the convergence of ransomware, cyber insurance and organisational cyber resilience. If the Committee would like further written details, we would be delighted to engage further.

16 December 2022

References:

Ioannis Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. Journal of Cybersecurity 4, no. 1. https://doi.org/10.1093/cybsec/tyy006.

Jamie MacColl, Jason R.C. Nurse and James Sullivan. 2021. Cyber Insurance and the Cyber Security Challenge. RUSI Occasional Paper. https://static.rusi.org/247-op-cyber-insurance-fwv.pdf

Jamie MacColl, Pia Hüsch and Jason R.C. Nurse. 2022, Beyond the Bottom Line: The Societal Impact of Ransomware. https://rusi.org/explore-our-research/publications/commentary/beyond-bottom-line-societal-impact-ransomware

Jason R.C. Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith & Sadie Creese. 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) (pp. 1-8). IEEE. https://kar.kent.ac.uk/80965/