Law Society of England and Wales and Bar Council joint response to the Home Office Consultation on Ransomware: proposals to increase incident reporting and reduce payments to criminals

April 2025

Introduction

1. The Law Society is the independent professional body for solicitors in England and Wales. We are run by our members, and our role is to be the voice of solicitors, to drive excellence in the profession and to safeguard the rule of law. As the body representing solicitors and with a statutory public interest role, part of the Law Society's overarching purpose is to safeguard the rule of law in the best interests of the public and the client. We are driven by our core objectives to promote access to justice, safeguard the rule of law, promote diversity and inclusion, the international practice of law and to support our members' businesses.

2. The Bar Council is the voice of the barrister profession in England and Wales. We lead, represent and support the Bar in the public interest, championing the rule of law and access to justice. Our nearly 18,000 members – self-employed and employed barristers – make up a united Bar that aims to be strong, inclusive, independent and influential. As the General Council of the Bar, we're the approved regulator for all practising barristers in England and Wales. We delegate our statutory regulatory functions to the operationally independent Bar Standards Board (BSB) as required by the Legal Services Act 2007.

3. We welcome the opportunity to jointly respond to the Home Office's consultation on ransomware. Our submission underscores the importance of increasing the cybersecurity posture for solicitors, barristers, the legal profession, and for the public. Ransomware is a serious threat to the legal sector, as outlined in the National Cyber Security Centre report on cyber threats on the UK legal sector, published in association with the Law Society, Bar Council, and other legal sector organisations.[1] We recognise that law firms and chambers are targets for the ever-growing threats from cyber criminals, and as part of our Law Society and Bar Council Joint Cybersecurity Working Group, have worked to support improved cybersecurity arrangements for the

[1] https://www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf

profession, such as through the development of a cybersecurity questionnaire and affirmation.[2]

Q10. To what extent do you agree, or disagree, that HMG should implement a targeted ban on ransomware payments for CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government.

4. We neither agree nor disagree about Proposal 1 being put forward by government about a targeted ban on ransomware payment. While we agree with the government and the evidence put forward by the public around the importance of breaking the cycle of ransomware payments being made by individuals and organisations, whether ransoms should be paid must be made on a case-by-case basis, often with existing contractual and external factors at play.

5. On paper, it may be possible to ban ransom payments, however as noted in the consultation paper, in practice, this may mean the closure of business functions or complete operations, particularly for critical services and infrastructures, and contravene existing business continuity plans. While there is no guarantee that payment of ransoms can ensure full recovery of data and systems, this may disproportionately affect individuals in need who can no longer access the necessary services, including access to legal services as well as court and tribunal services.

6. If departments and organisations have cyber insurance policies in place, whether a ransom should be paid will be dependent on the terms of such insurance, as well as the potential costs and data that may be recovered. From the legal profession's perspective, should the government plan to ban ransom payments, these cyber insurance policies will need to be amended, with potential wider reaching impact of terms of services and contractual obligations, as well as professional obligations as relevant to client confidentiality and their data.

7. Proposals to ban ransom payments may also increase the likelihood of cyber attacks on the private sector and other organisations not covered by the ban. As a result, while the focus of the proposal is on the public sector, wider consideration of the sectoral and industry landscape must be thought through to ensure that there are no cascading effects of cyber risk mitigation. Fundamentally, the private sector's property rights are their own, and so bans on ransom payments should be restricted to the public sector. Any change to the current regime needs to be evidence-based, and in active consultation with stakeholders across the public and private sectors.

Q11. How effective do you think this proposed measure will be in reducing the amount of money flowing to ransomware criminals, and thus reducing their income?

8. Neither effective nor ineffective, where there is insufficient evidence to make a judgement.

---

[2] https://www.lawsociety.org.uk/contact-or-visit-us/press-office/press-releases/law-firms-and-chambers-working-together-to-improve-cybersecurity; https://www.barcouncil.org.uk/bar-council-services/for-chambers-and-aetos/cybersecurity-questionnaire.html

Q12. How effective do you think banning CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, from making a payment will be in deterring cyber criminals from attacking them?

9. Somewhat effective, where there is insufficient evidence to make a concrete judgement.

Q13. What measures do you think would aid compliance with the proposed ban?

10. Additional guidance to support compliance with the ban.

11. Tailored support to manage the response and impact following an attack.

Q14. What measures do you think are appropriate for non-compliance with the proposed ban?

12. Civil penalties for non-compliance.

Q15. If you represent a CNI organisation or public sector body, would your organisation need additional guidance to support compliance with a ban on ransomware payments?

13. Not applicable.

Q16. Should organisations within CNI and public sector supply chains be included in the proposed ban?

14. Don't know.

Q17. Do you think there should be any exceptions to the proposed ban?

15. Don't know.

Q18. Do you think there is a case for widening the ban on ransomware payments further, or even imposing a complete ban economy-wide (all organisations and individuals)?

16. No. As noted in our response to Q10, we believe that careful consideration needs to be made to the external factors and wider implications of a ban for both the public sector and economy. While we agree that payment of ransoms does not guarantee data or financial recovery, increasing the robustness of cyber posture remains fundamental to preventing ransomware attacks, prior to decisions around ransomware payment.

Q19. To what extent do you agree, or disagree, that the Home Office should implement the following:

17. We strongly disagree on an 'Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.'

18. We tend to disagree on a 'Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.'

19. We tend to disagree on a 'Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.'

20. We tend to disagree on a 'Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.' We do not believe that individuals should be included in the ransomware payment prevention regime due to the undue burden placed on them. This extends to SMEs and small amounts of ransom demanded. We agree that more information on the ransomware landscape would help the government tackle cyber crime, but reporting requirements and disclosure should be proportionate to the measurable gain achieved from the prevention regime. As noted, there are already existing disclosure requirements to data and information breaches, and further requirements for disclosure, particularly within the short timeframes proposed, would be onerous to comply with.

Q20. How effective do you think the following will be in reducing ransomware payments?:

21. We believe an 'Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1' will be somewhat ineffective.

22. We believe a 'Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1' will be somewhat ineffective.

23. We believe a 'Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals' will be somewhat ineffective.

24. We believe a 'Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals' will be somewhat ineffective.

Q21. How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors?:

25. We believe an 'Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1' will be somewhat effective.

26. We believe a 'Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1' will be somewhat effective.

27. We believe a 'Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals' will be somewhat effective.

28. We believe a 'Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals' will be somewhat effective.

Q22. If we introduced a threshold-based payment prevention regime, what would be the best way to determine the threshold for inclusion?

29. We believe that consideration of an organisation's annual turnover in the UK, organisation's number of employees in the UK, sector, amount of ransom demanded, would all be useful considerations for determining the threshold for inclusion. However, this must only be an initial assessment of inclusion with the regime, subject to further assessment of feasibility to compliance with the regime based on business and operational demands as well as sector-specific responsibilities and obligations. Implementing thresholds may also encourage cybercriminals and others to work around them, potentially introducing unintended negative consequences.

Q23. What measures do you think would aid compliance with a payment prevention regime?

30. We believe that additional guidance to support compliance and support to manage the response and impact following an attack are essential.

Q24. Do you think these compliance measures need to be tailored to different organisations and individuals?

31. Yes, compliance measures must be tailored to respond to specific cases, sectoral approaches, and ensure that there is no undue burden for SME organisations.

Q25. What measures do you think are appropriate for non-compliance with a payment prevention regime?

32. Civil penalties for non-compliance.

Q26. Do you think these non-compliance measures need to be tailored to different organisations and individuals?

33. Yes, non-compliance measures must be tailored to respond to specific cases, sectoral approaches, and ensure that there is no undue burden for SME organisations.

Q27. For those reporting on behalf of an organisation, who do you think should be legally responsible for compliance with the regime?

34. The organisation.

Q28. For those reporting on behalf of an organisation, do you think any measures for managing non-compliance with the regime should be the same for both the organisation and a named individual responsible for a ransomware payment?

35. Yes.

Q29. To what extent do you agree, or disagree, that the Home Office should implement the following:

36. We strongly agree on the 'Continuation of the existing voluntary ransomware incident reporting regime.'

37. We strongly disagree on the 'Economy-wide mandatory reporting for all organisations and individuals.'

38. We strongly disagree on 'Threshold-based mandatory reporting, for certain organisations and individuals.'

39. We strongly disagree on 'Mandatory reporting for all organisations excluding individuals.'

40. We tend to agree on 'Threshold-based mandatory reporting, for certain organisations excluding individuals.' Where the ransom may be a significant amount, we tend to agree that there should be organisation-based reporting.

41. For both the legal profession and the professional services industry, a fundamental question when reporting and for ransomware payments is considering what services, systems, and data may have been lost. There may be significant reputational damage should a cyber attack such as ransomware be disclosed and so any reporting regime must be secure, anonymous, as well as have a clearly defined purpose. Within the legal sector, we are aware of voluntary networks and groups of organisations and their cybersecurity functions sharing threat intelligence to enable quick reactions and responses which may support protection, already taking direct action to minimise organisational damage. Delayed reporting without public disclosure to the National Cyber Security Centre (NCSC) may offer the government the opportunity to provide public information on current and potential threats. As noted in Q22, implementing thresholds may complicate reporting and incentivise bad actors to work below the established threshold, potentially introducing unintended consequences regarding ransomware as well as the ransomware payments regime.

Q30. How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK?:

42. We believe the 'Continuation of the existing voluntary ransomware incident reporting regime' would be somewhat effective.

43. We believe 'Economy-wide mandatory reporting for all organisations and individuals' would be somewhat effective.

44. We believe 'Threshold-based mandatory reporting, for certain organisations and individuals.' would be effective.

45. We believe 'Mandatory reporting for all organisations excluding individuals' would be effective.

46. We believe 'Threshold-based mandatory reporting, for certain organisations excluding individuals' would be effective.

Q31. How effective do you think the following would be in increasing the Government's ability to tackle and respond to the ransomware threat to the UK?:

47. We believe the 'Continuation of the existing voluntary ransomware incident reporting regime' would be somewhat effective.

48. We believe 'Economy-wide mandatory reporting for all organisations and individuals' would be neither effective nor ineffective.

49. We believe 'Threshold-based mandatory reporting, for certain organisations and individuals' would be somewhat effective.

50. We believe 'Mandatory reporting for all organisations excluding individuals' would be somewhat effective.

51. We believe 'Threshold-based mandatory reporting, for certain organisations excluding individuals' would be somewhat effective.

Q32. If we introduced a mandatory reporting regime for victims within a certain threshold, what would be the best way to determine the threshold for inclusion?

52. We believe that consideration of an organisation's annual turnover in the UK, organisation's number of employees in the UK, sector, amount of ransom demanded, would all be useful considerations for determining the threshold for inclusion. As noted above, implementing thresholds may also encourage cybercriminals and others to work around them, potentially introducing unintended negative consequences.

Q33. What measures do you think would aid compliance with a mandatory reporting regime?

53. We believe that additional guidance to support compliance and support to manage the response and impact following an attack are essential.

Q34. Do you think these compliance measures need to be tailored to different organisations and individuals?

54. Yes, compliance measures must be tailored to respond to specific cases, sectoral approaches, and ensure that there is no undue burden for SME organisations.

Q35. What measures do you think are appropriate for non-compliance with a payment prevention regime?

55. Civil penalties for non-compliance.

Q36. Do you think these non-compliance measures need to be tailored to different organisations and individuals?

56. Yes, non-compliance measures must be tailored to respond to specific cases, sectoral approaches, and ensure that there is no undue burden for SME organisations.

Q37. Do you think the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors?

57. Yes, a mandatory incident reporting regime would impact business decisions given the shift in potential risk and risk management processes, as well as required disclosure of data.

Q38. For mandatory reporting regime, is 72 hours a reasonable time frame for a suspected ransomware victim to make an initial report of an incident?

58. Don't know, as it is unclear what information is necessary as part of this initial report. We believe that it is unlikely that 72 hours will be a reasonable time frame given the necessary information needed for such a report to be useful in the first instance.

Q39. Do you think that an incident reporting regime should offer any of the following services to support victims when reporting?

59. We believe that support from cyber experts such as the NCSC or law enforcement, guidance documents, threat intelligence on ransomware criminals and trends, and operational updates such as activities law enforcement are undertaking would all be useful services to support victims when reporting.

Q40. Should mandatory reporting cover all cyber incidents (including phishing, hacking etc.) rather than just ransomware?

60. No.