Consultation Options Assessment

Title:	Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting.
Type of measure:	Primary legislation
Department or agency:	The Home Office
OA number:	HO COA 1002
RPC reference number:	
Contact for enquiries:	ransomwareconsultation@homeoffice.gov.uk
Date:	14/01/2025

Contents

1. Summary of proposal 3
2. Strategic case for proposed regulation 4
3. SMART objectives for intervention 13
4. Description of proposed intervention options and explanation of the logical change process whereby this achieves SMART objectives 15
5. Summary of long-list and alternatives 17
6. Description of shortlisted policy options carried forward 18
7. Monitoring and evaluation 22
8. Minimising administrative and compliance costs 23
Declaration 24
Summary: Analysis and evidence 25
Annex 28
Evidence Base 28
Appraisal 28
Option 0: Do Nothing 36
Option 1: A complete ban on ransomware payments. 36
Option 2: A targeted ban on ransomware payments for regulated CNI and the public sector 39
Option 3: A ransomware payments prevention regime for all other ransomware payments. 41
Option 4: Mandatory reporting of a payment prior to the transaction 44
Option 5: A mandatory reporting regime for all sectors. 47
Option 6: Mandatory reporting of ransomware incidents for specific sectors 50
Overall Costs and Benefits 53
Statutory Equalities Duty 57

1. Summary of proposal

1. Ransomware is considered a risk to the UK's national security by the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC). Ransomware poses the greatest serious and organised cyber crime threat, and the largest cyber security threat to the UK.

2. For the purpose of the consultation, the Home Office views ransomware as: a type of malicious software ("malware") that infects a victim's computer system(s). It can prevent the victim from accessing system(s) or data, impair the use of system(s) or data and/or facilitate theft of data held on the victim's networked systems or devices. A ransom is demanded (normally payment of cryptocurrency) from the victim to regain access to the system(s); for data to be restored; or for data not to be published on criminal-operated data leak websites.[1]

3. The Home Office proposes to introduce legislation to counter ransomware and meet three main objectives:
   - Reduce the amount of money flowing to ransomware criminals from the UK, thereby deterring criminals from attacking UK organisations.
   - Increase the ability of operational agencies to disrupt and investigate ransomware actors by increasing our intelligence around the ransomware payment landscape.
   - Enhance the government's understanding of the threats in this area to inform future interventions, including through cooperation at international level.

4. The Home Office is seeking consultation feedback on the following proposals, options are explained in detail in Section 6: Description of shortlisted policy options carried forward:

   Option 0: Do Nothing.

   Option 1: A complete ban on ransomware payments.

   Option 2: A targeted ban on ransomware payments for regulated Critical National Infrastructure (CNI) and the public sector.

   Option 3: A ransomware payments prevention regime for all ransomware payments.

   Option 4: Mandatory reporting of a payment prior to the transaction (sector specific or economy wide).

   Option 5: A mandatory ransomware incident reporting regime for all sectors.

   Option 6: Mandatory reporting of ransomware incidents for specific sectors.

5. The evidence from this consultation will also support future advice and guidance that the Home Office intends to produce for the victims of ransomware.

[1] This includes but is not limited to encryption.

2. Strategic case for proposed regulation

What is the problem under consideration?

6. Evidence in relation to ransomware is set out in the published consultation document[2] and for ease, is summarised again here.

7. Ransomware is considered the greatest serious and organised cyber crime threat, the largest cyber security threat and a risk to the UK's national security by the NCA and the NCSC.

8. This is demonstrated by the increase in ransomware incidents, which are continuing an upward trend. In 2023, incidents of ransomware attacks reported to the Information Commissioner's Office (ICO) reached their highest level since 2019[3] and private sector reporting to the NCA indicates the number of UK victims appearing on ransomware data leak sites has doubled since 2022.[4] This is reflected globally, with industry estimates suggesting that in 2023 ransomware criminals received at least $1 billion[5] in ransom payments. These attacks are increasingly sophisticated and affect organisations across the entire economy.

9. Ransomware is of widespread concern to the public, with 2024 polling commissioned by the Home Office showing that nearly three quarters (74%) of the public were concerned about the possibility of ransomware occurring in the UK.[6]

10. The NCA describes ransomware as one of the most harmful cyber threats due to: the significant financial losses incurred, the theft of intellectual property, sensitive commercial data, or customer Personally Identifiable Information (PII), disruption of service, and reputational harm that can result. Associated data breaches can also cause serious harm to individuals and, when considered collectively, represent a systemic risk to UK society and the UK economy.[7]

11. The NCSC assess that ransomware is a financially motivated crime, largely committed by cyber criminals.[7] These criminals are assessed by NCSC to be predominantly based overseas, in Russia and other jurisdictions that do not routinely cooperate with UK law enforcement. They are not typically directed by their host states but operate as part of organised crime groups or networks.[8] These criminals can impact the UK's most critical infrastructure and services, meaning ransomware poses a significant threat to the UK's national security.

12. These financially motivated cyber criminals seek to maximise their profits through large scale attacks. Academic research suggests that these criminals trade off the probability and willingness of a victim to pay against increasing the ransom and the subsequent

---

[2] Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting. Government consultation. (Home Office, 2025)

3 Data security incident trends | ICO. https://ico.org.uk/action-weve-taken/data-security-incident-trends/

[4] NCA National Strategic SOC Assessment 2024, https://www.nationalcrimeagency.gov.uk/nsa-overview-of-soc-2024

[5] Ransomware Hit $1 Billion in 2023 (chainalysis.com), https://www.chainalysis.com/blog/ransomware-2024/

[6] Home Office, in collaboration with Ipsos 'Knowledge and perceptions of the UK public on ransomware against businesses' (2025).

[7] Ransomware, extortion and the cyber crime ecosystem (NCA, NCSC), https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem#section_2

[8] Foreign Secretary issues warning to Russia on ransomware - BBC News, https://www.bbc.co.uk/news/technology-57084943#:~:text=Those%20educational%20institutions%20hit%20by%20ransomware%20earlier%20this,issued%20a%20series%20of%20alerts%20on%20the%20issue

profit. Criminals may refine their techniques and learn better strategies to maximise profit, for example, through offering victims a range of options at different prices or giving different victims different prices.[9] The perception that a victim will pay the ransom demanded is a key factor in a criminals' decision to invest time and resources in instigating an attack. The UK has an opportunity to try to change these perceptions.

13. There are many business models available to ransomware actors, but the most common business model is 'Ransomware as a Service' (RaaS). In this model, organised crime groups provide other cyber criminals with malware to orchestrate an attack anonymously for a cut of the ransom payment. The introduction of RaaS has lowered barriers to entry and makes it possible for any criminal to cause widespread harms without advanced technical skills.[10]

Evidence to support the problem statement, the impact of ransomware

14. Academic research based on interviews with victims and incident reporters has highlighted the wide range of harms caused by ransomware. This includes physical, financial, reputational, psychological, and social harms.[11] In some cases, the significant financial costs and losses experienced by organisations can threaten their existence, with public reports highlighting instances of organisations permanently ceasing to trade following a ransomware attack.

15. As examples, in September 2023, KNP Logistics Group (the UK's largest logistics company) blamed a ransomware attack suffered three months earlier for its insolvency, with the loss of more than 700 jobs in the process.[12]

16. Foreign exchange firm, Travelex, collapsed into administration six months after a ransomware attack at the end of 2019, with administrators citing the impact of the attack as a key contributing factor.[13]

17. Academic research also highlights that ransomware not only has a direct impact on the targeted organisation and its staff, but can impact indirectly on other organisations and individuals, with a cumulative effect of incidents on wider society, the economy and national security.[14]

18. Academic estimates of unlikely yet possible worst-case attacks can illustrate the possible scale of ransomware harms to the UK. A scenario-based model by the Cambridge Centre for Risk Studies analysed possible harms of an attack on UK critical national infrastructure via the South East electricity distribution network. Due to lost

[9] An economic analysis of ransomware and its welfare consequences | Royal Society Open Science (royalsocietypublishing.org), https://royalsocietypublishing.org/doi/10.1098/rsos.190023
[10] Ransomware, extortion and the cyber crime ecosystem (ncsc.gov.uk). https://www.ncsc.gov.uk/pdfs/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem.pdf
[11] Ransomware: Victim Insights on Harms to Individuals, Organisations and Society | Royal United Services Institute (rusi.org), https://www.rusi.org/explore-our-research/publications/occasional-papers/ransomware-victim-insights-harms-individuals-organisations-and-society
[12] UK logistics firm blames ransomware attack for insolvency, 730 redundancies (therecord.media), https://therecord.media/knp-logistics-ransomware-insolvency-uk
[13] Travelex falls into administration, with loss of 1,300 jobs | Job losses | The Guardian, https://www.theguardian.com/business/2020/aug/06/travelex-falls-into-administration-shedding-1300-jobs
[14] Ransomware: Victim Insights on Harms to Individuals, Organisations and Society | Royal United Services Institute (rusi.org), https://www.rusi.org/explore-our-research/publications/occasional-papers/ransomware-victim-insights-harms-individuals-organisations-and-society

power, the report calculated sector direct losses to production of between £7.2 billion and £53.6 billion, with a central estimate of £18.1 billion based on response time.[15]

19. The report scenario is not ransomware specific, instead focussing on the possible impacts of wider malicious cyber activity. Whilst it cannot necessarily be directly extrapolated to a ransomware attack, it provides a useful possible magnitude of a worst-case scenario.

20. These harms can be exacerbated when there are impacts on supply chains or a loss in trust of law enforcement and public services. In-depth interviews[16] exploring the experience and impacts of ransomware attacks with individual and business victims found that they suffered both financial and non-financial costs. Financial costs were both direct and indirect, with some organisations needing to pay significant amounts for external technical, legal or PR support. There can also be high costs for the closure or disruption of services.

21. Another example of the impacts of ransomware attacks is demonstrated by the 2024 ransomware attack on Synnovis, a pathology service joint NHS-private venture.[17] Disruption of IT services led to elective surgeries being cancelled, patient services (including cancer treatments) being disrupted, and some services having to be diverted to other hospitals.[18] Up to 26 September 2024, NHS data showed 10,152 acute outpatient appointments and 1,710 elective procedures were postponed at King's College Hospital NHS Foundation Trust and Guy's and St Thomas' NHS Foundation Trust, as a result of the disruption.[19]

22. As well as profiting from the payment of ransoms, academic research indicates that criminals can either directly sell the data that they steal in online marketplaces[20] or use it themselves for a range of malicious purposes. This can include card-not-present fraud, digital identify theft, the creation of false accounts, or breaking a password or username recovery process to takeover an existing digital or bank account.[21]

23. Many organisations have increased the volume and type of data they collect on their customers to feed proprietary algorithms (including behavioural, attitudinal, and engagement data, and sometimes tracking and real-time location data). As a result, the theft and onward sale of this data to other criminals or states can facilitate serious crime and harm to individuals, including threats to life, and a systemic risk to society.[22, 23]

---

[15] Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf

[16] Home Office in collaboration with Ipsos 'The experiences and impacts of ransomware attacks on individuals and businesses' (2025).

[17] https://www.synnovis.co.uk/cyberattack-information-centre

[18] The Scourge of Ransomware: Victim Insights on Harms to Individuals, Organisations and Society (rusi.org), https://static.rusi.org/ransomware-harms-op-january-2024.pdf

[19] NHS England: Clinical impact in south east London, https://www.england.nhs.uk/london/2024/09/26/update-on-cyber-incident-clinical-impact-in-south-east-london-thursday-26-september-2024/

[20] Ouellet *et al*. (2022) 'The network of online stolen data markets: How vendor flows connect digital marketplaces', https://academic.oup.com/bjc/article/62/6/1518/6503727

21 Zaeifi *et al*. (2024) 'Nothing personal: Understanding the spread and use of Personally Identifiable Information in the Financial Ecosystem', https://dl.acm.org/doi/10.1145/3626232.3653266

[22] Ablon (2018) Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data Rand, https://www.rand.org/pubs/testimonies/CT490.html

[23] Curran (2023) 'Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness', https://journals.sagepub.com/doi/full/10.1177/20539517231177621

24. There are potential long-term risks associated with online security complacency and data privacy fatigue.[24] Academic research suggests that as ransomware attacks (and associated data breaches) become more frequent, the more the public loses confidence in government and begins to believe such crimes are an inevitable part of living their lives online.[25]

25. Home Office polling[26] suggests that the UK public are aware of some of these additional impacts. The public were presented with a range of scenarios regarding the payment of a ransom, including what might happen in the event of payment. 68 per cent of the public believed that it is wrong for a business to pay a ransom because that ransom could be used by attackers to fund more criminal activities. Wider research has found that the proceeds of these crimes are largely transferred through cryptocurrency, which has made purchasing criminal services and receiving payments easier, cheaper, and faster. This creates challenges in identifying individuals and controlling illicit payments.[27]

26. The continued use and adaptation of ransomware methods suggests that criminals view this as a profitable activity. The financial incentive to continue ransomware attacks is unlikely to reduce. The financial incentive could grow as digitalisation continues, as organisations of all kinds store more valuable data that can be targeted and extorted. The combined challenges of overseas impunity, anonymity and traceability of finance makes ransomware very difficult to prosecute, disrupt and reduce through law enforcement.

27. Law enforcement have evolved their response to ransomware attacks and the cyber crime ecosystem and have delivered significant success such as the 2024 disruption against the LockBit ransomware group[28]. Examples of these successes are outlined in more detail in the published consultation document. The government uses all the tools at its disposal to target these criminals, and to date has sanctioned 36 Russian individuals who have been responsible for some of the most serious ransomware attacks against the UK and allies.[29]

Evidence to support the problem statement, ransomware incidents and victimisation

28. There is some evidence available on the scale of ransomware within the UK, against both individuals and organisations. The ICO receives reports of data security breaches within 72 hours of discovery and these reports include ransomware incidents experienced by organisations. The data in the graph below from the ICO suggests that incidents of ransomware attacks are increasing, with ransomware incidents reported to the ICO peaking at 511 in the second quarter of 2023[30].

---

[24] Choi, Park, and Jung (2018) 'The role of privacy fatigue in online privacy behaviour', https://www.sciencedirect.com/science/article/abs/pii/S0747563217306817

[25] Shandler and Gomez (2022) 'The hidden threat of cyber-attacks – undermining public confidence in government'. https://www.tandfonline.com/doi/full/10.1080/19331681.2022.2112796

[26] Home Office in collaboration with Ipsos 'Knowledge and perceptions of the UK public on ransomware against businesses' (2025).

[27] Ransomware, extortion and the cyber crime ecosystem - NCSC.GOV.UK, https://www.ncsc.gov.uk/whitepaper/ransomware-extortion-and-the-cyber-crime-ecosystem

[28] Over a four-year period from 2020-24, the Russian-based LockBit organisation became the most prolific and harmful facilitator of ransomware attacks worldwide, targeting thousands of victims and causing losses of billions in ransom payments and recovery costs. Their main business was selling so-called 'affiliates' the tools and infrastructure required to carry out their own attacks, a practice known as ransomware-as-a-service (RaaS).

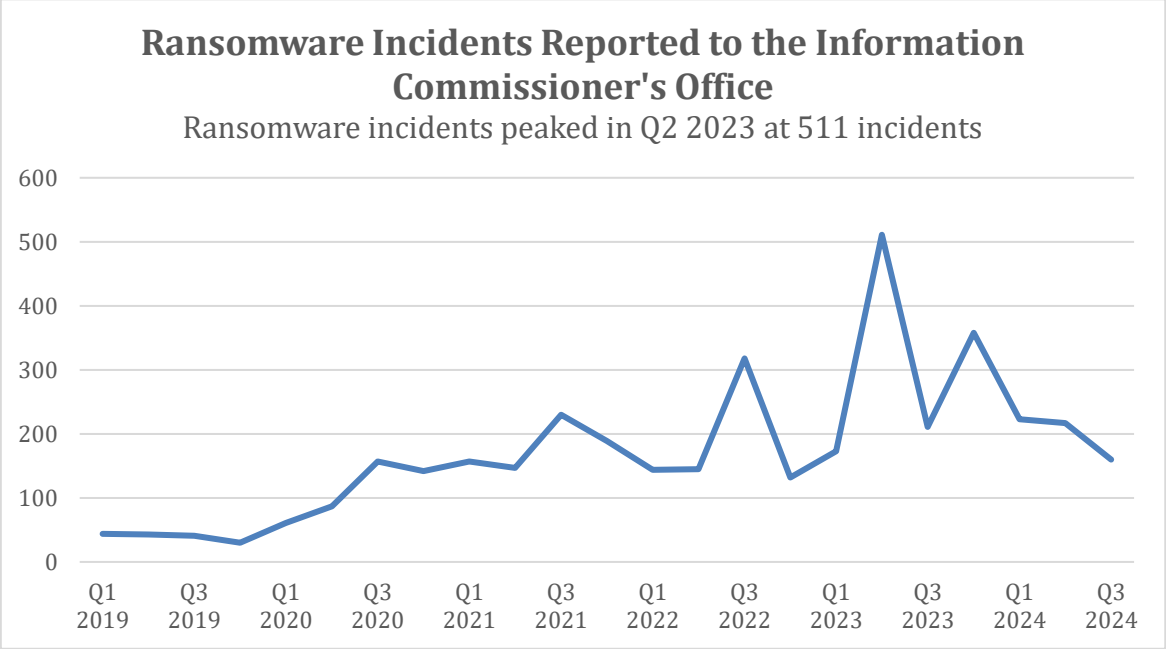
[29] The UK Sanctions List, https://search-uk-sanctions-list.service.gov.uk/

[30] Data security incident trends | ICO, https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Table 1: Ransomware Incidents Reported to the Information Commissioner's Office per quarter, 2019 Q1 to 2024 Q3.

Year	Quarter	Number of incidents
2019	Q1	44
2019	Q2	43
2019	Q3	41
2019	Q4	30
2020	Q1	61
2020	Q2	87
2020	Q3	157
2020	Q4	142
2021	Q1	157
2021	Q2	147
2021	Q3	230
2021	Q4	189
2022	Q1	144
2022	Q2	145
2022	Q3	318
2022	Q4	132
2023	Q1	173
2023	Q2	511
2023	Q3	211
2023	Q4	358
2024	Q1	223
2024	Q2	217
2024	Q3	160

Source: Information Commissioner's Office



Source: Information Commissioner's Office

29. Wider evidence on the scale of ransomware attacks is limited due to factors such as underreporting of cyber crime and the sophisticated nature of ransomware attacks. However, other evidence gives some indication of the extent of victimisation:

- Private sector reporting to the NCA indicates the number of UK victims appearing on ransomware data leak sites has doubled since 2022.[31]
- The Cyber Security Breaches Survey (CSBS, 2024),[32] focusses on the cost and impact of cyber breaches and attacks on businesses, charities, and educational institutions. The CSBS found that among the 50 per cent of businesses that reported experiencing at least one cyber-attack, 6 per cent of businesses identified their organisation's devices being targeted with ransomware.[33]
- The Crime Survey for England and Wales[34] in the year to March 2023, estimated there was a demand for money to release files in three per cent of computer virus incidents against individuals in the year to March 2023, it should be noted this is only a proxy indicator for ransomware against individuals.
- Home Office polling with the UK general public[35] also suggested that approximately 11 per cent of the public had indirect experience of ransomware, reporting that the organisation where they work or an organisation they are a customer of had experienced a ransomware attack.

[31] NCA National Strategic Assessment, 2024, https://www.nationalcrimeagency.gov.uk/nsa-2024
[32] Cyber security breaches survey 2024 - GOV.UK (www.gov.uk), https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024
[33] Cyber security breaches survey 2024 - GOV.UK (www.gov.uk), https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024
[34] Crime in England and Wales - Office for National Statistics (ons.gov.uk), https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023
[35] Home Office in collaboration with Ipsos 'Knowledge and perceptions of the UK public on ransomware against businesses' (2025).

30. Specific examples of recent UK ransomware incidents that highlight the need to take further steps to combat this threat include:

- **NHS Dumfries & Galloway (March 2024),** a ransomware group posted three terabytes of stolen patient data on the dark web.
- **British Library (October 2023)**, a ransomware group posted approximately 600GB of stolen staff data on the dark web following the cyber-attack. Research services were severely restricted for two months, with full recovery continuing for longer.[36]
- **Capita breach (March 2023),** this ransomware incident compromised sensitive data affecting pensions nationwide. Capita reported that they expected associated costs to be around £15 million to £20 million.[37]
- **Royal Mail ransomware attack (January 2023)**, domestic and international operations were affected for several weeks when attacked by the Russian affiliated cyber-crime group LockBit.
- **Redcar and Cleveland local council attack (February 2020),** this attack left around 135,000 people without online access to public services and the local council was unable to take in any payments following its cyber-attack.[38] Redcar and Cleveland local council estimate their losses to be around £8.7 million.[39]

Why is government intervention necessary, policy rationale

31. Legislation is a necessary step to transform the UK's approach and reduce the threat of ransomware. The Home Office wants to undermine the ransomware business model and disrupt the criminal actors. It ultimately aims to make the UK a less attractive target for ransomware and cyber-attacks generally.

32. Currently, the UK has no ransomware-specific legislation. However, the UK led a non-binding international statement through the Counter Ransomware Initiative (CRI) in 2023, which saw 40 CRI members and 8 global insurance bodies agree that "relevant institutions" under their governments would not make ransomware payment.[40]

33. The UK's main cyber crime legislation, the Computer Misuse Act 1990,[41] is currently being reviewed. However, the Home Office judges that the nature and scale of the ransomware threat requires the development of new targeted legislative interventions.

34. The government will be introducing other cyber-related legislation and the Home Office is working closely with Lead Departments to understand where any deconfliction may be required and ensure proportionality in our approach, particularly for Critical National Infrastructure.

---

[36] British Library cyber incident review, March 2024 - https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf, https://www.bl.uk/home/british-library-cyber-incident-review-8-march-2024.pdf

[37] Capita, May 2023. Update on cyber incident | Capita, https://www.capita.com/news/update-actions-taken-resolve-cyber-incident

[38] committees.parliament.uk/oralevidence/12620/pdf/, https://committees.parliament.uk/oralevidence/12620/pdf/

[39] Cost of Redcar Council cyber-attack over-estimated - BBC News, https://www.bbc.co.uk/news/uk-england-tees-57433800

[40] CRI joint statement on ransomware payments, https://www.gov.uk/government/publications/cri-joint-statement-on-ransomware-payments/cri-joint-statement-on-ransomware-payments

[41] Computer Misuse Act 1990 (legislation.gov.uk). https://www.legislation.gov.uk/ukpga/1990/18/contents

35. The combination of overseas impunity, anonymity and untraceable finance makes ransomware very difficult to prosecute and reduce through regular law enforcement. The continued use and adaptation of ransomware methods suggests that criminals view this as a profitable activity. The financial incentive to continue ransomware attacks is unlikely to reduce and it could grow as digitalisation continues.

36. A main objective of these legislative proposals is to disrupt the criminal business model that ransomware actors benefit from. By acting as a deterrent and increasing public and government awareness of incident, the government hopes to get ahead of the problem.

37. Ransomware criminals have proven highly adaptive, and the Home Office anticipates that further technological enablers such as artificial intelligence and quantum computing will enhance the future threat from ransomware. This increases the urgency to act now to disrupt the criminal business model.

38. Reducing money flowing to ransomware criminals can disrupt their capacity to build and sustain their capabilities, and reduce the threat posed to UK organisations. Effort put into attacks which do not lead to payment are unattractive propositions for ransomware criminals.

39. Changing the regulatory and legal environment around the reporting of, and payment of, ransomware demands could change the overall vulnerability of the UK to ransomware. By restricting ransomware payments, the government aims to position the UK, and particularly CNI, as an unattractive prospect to criminals, with a reputation that the UK does not pay.

40. There is no clear answer to the threat of ransomware, either across domestic stakeholders or international counterparts. Some international counterparts are leading the way with new laws and regulations. The USA, Australia and France all have varying degrees of mandatory cyber incident reporting regimes for ransomware. The UK can learn from and improve on these models, addressing the threat in a manner tailored to the UK legal, economic, and technical context.

41. The Home Office recommends a package of interventions supported by a comprehensive communications approach, ongoing industry engagement and voluntary measures. While building on existing precedents from US and Australian cyber legislation, the proposals set out in section 1, paragraph 4 of this OA, address the specific motivations to disrupt the ‘for profit’ model of ransomware criminals.

Why is government intervention necessary, economic rationale

42. Ransomware is a financially motivated and extortive form of cyber crime. The profit generated for criminals is only possible if a victim’s behaviour exhibits a willingness to pay. The highly sophisticated criminal enterprise surrounding the RaaS model is not encouraged by successful attacks in themselves, but from eventual payment. Potential changes to victim behaviour offer a major interference point in the ransomware business model.

43. It is expected that by banning ransomware payments, the number of ransomware attacks will eventually decrease due to the lack of monetary incentive. This would reduce the cost to the UK economy from ransomware through lower recovery and disruption costs for targeted UK organisations.

44. Industry research in 2023 found that globally it is not always advantageous for firms to pay ransom demands. Businesses who paid a ransom experienced only a small difference in total cost at USD 5.06 million compared to USD 5.17 million, a cost difference of USD 0.1 million or 2.2 per cent. However, this calculation doesn't include the cost of the ransom itself. Given the high cost of most ransomware demands, organisations that paid the ransom likely ended up spending more overall than those that did not pay the ransom.[42]

45. Industry research in 2022 found the total cost savings were USD 0.63 million, with a total cost difference of 13.1 per cent, again not including the cost of the ransom itself. Industry research suggests that paying a ransom has become increasingly less advantageous overall, with an 82.5 per cent decrease in savings from 2022 to 2023.[43]

46. There is an economic rationale for government intervention banning ransomware payments, either for the full business population or for the CNI sector, as it will reduce the flow of money from legal UK business to ransomware criminals. Payments to ransomware criminals represent a loss to the UK economy and fund wider criminality.

47. Government intervention mandating ransomware reporting reduces the information asymmetry between ransomware criminals and UK law enforcement around the scale and nature of ransomware. This will allow UK law enforcement to better disrupt and investigate ransomware criminals through increased visibility and knowledge of the ransomware payment landscape.

48. The introduction of a mandatory reporting regime directly plugs the gap in reporting and intelligence gathering between ransomware victims and UK law enforcement and introduces a novel approach of reporting and monitoring criminal and hostile actor activity with an impact to the UK.

[42] Cost of a data breach 2024 | IBM, https://www.ibm.com/reports/data-breach
[43] Cost of a data breach 2024 | IBM; https://www.ibm.com/reports/data-breach

3. SMART objectives for intervention

What are the policy objectives of the intervention and the intended effects?

49. The overall motivation for the proposed interventions is to reduce cyber crime and the associated harms to UK businesses, reducing the threat of ransomware attacks by making the UK a less attractive target to ransomware criminals. Simultaneously, the Home Office is looking to shore up the most crucial parts of the UK economy, reducing the national security threat that ransomware poses.

50. The Home Office seeks to achieve this by brigading the department's work through the following strategic objectives:
    - Reduce the amount of money flowing to ransomware criminals from the UK, thereby deterring criminals from attacking UK organisations.
    - Increase the ability of operational agencies to disrupt and investigate ransomware actors by increasing our intelligence around the ransomware payment landscape.
    - Enhance the government's understanding of the threats in this area to inform future interventions, including through cooperation at international level.

How do these objectives align with the government's objectives and policy objectives?

51. This activity is consistent with the UK's long standing cyber objectives, introduced by the previous government and specifically contributes to four main strategic objectives and international efforts to address the harm posed by ransomware:
    - The Home Office's Outcome Delivery Plan priority of reducing crime[44]
    - The government's Cyber Security Strategy[45]
    - The government's National Cyber Strategy 2022[46]
    - The Home Office's response to the National Security Strategy Joint Committee's (JCNSS) inquiry into Ransomware[47]
    - The Counter Ransomware Initiative (a global initiative committed to mitigating the impact of ransomware)[48]

52. **The National Cyber Strategy,** December 2022[49], details the UK's role as a responsible and democratic cyber power, protecting and promoting UK interests in, and through, cyberspace. The Home Office is the coordinating department for the Threat Pillar (V),

[44] The Home Office's Outcome Delivery Plan priority of reducing crime, https://www.gov.uk/government/publications/home-office-outcome-delivery-plan/home-office-outcome-delivery-plan-2021-to-2022#reduce-crime
[45] The Government's Cyber Security Strategy, https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030
[46] National Cyber Strategy 2022 - GOV.UK (www.gov.uk), https://www.gov.uk/government/publications/national-cyber-strategy-2022
[47] Ransomware - Committees - UK Parliament, https://committees.parliament.uk/work/7017/ransomware/
[48] CRI joint statement on ransomware payments - GOV.UK (www.gov.uk). https://www.gov.uk/government/publications/cri-joint-statement-on-ransomware-payments
[49] National Cyber Security Strategy 2022: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

which is jointly chaired by Home Office, FCDO and MOD. The strategy commits £2.6 billion of new investment to deliver objectives under five strategic pillars:

1) **Eco-System** - Strengthening the UK cyber ecosystem by investing in cyber skills, deepening partnerships between government, academia and industry, and strengthening UK cyber exports.
2) **Resilience** - Building a resilient and prosperous digital UK by reducing cyber risks to users, ensuring citizens feel safe online and confident that their data is protected.
3) **Technology** - Taking the lead in the technologies vital to cyber power by building our industrial capability and sustaining advantage in security technologies critical to cyberspace (including microprocessor design, operational technologies and cryptography).
4) **International** - Advancing UK global leadership and influence towards a more secure, prosperous and open international order, sharing the expertise that underpins UK cyber power.
5) **Threat** - Detecting, disrupting and deterring malign use of technology by our adversaries by using the UK's full set of levers in a more integrated and creative way.

53. Tackling cyber crime is central to this strategy. The Home Office coordinates policy, governance, and capabilities to reduce criminal computer misuse that impacts the UK. It aims to understand, detect, deter and disrupt the highest harm and highest impact cyber threats to domestic security.

Are there any other indicators of success that should be considered?

54. A reduction in repeat attacks on victims either by the same criminal or ransomware strand will allow the Home Office to measure success as an indicator of the UK's resilience, either to be able to: recover fully from the first attack and block subsequent attacks; or deter repeat attacks.

55. A reduction in payments to ransomware actors from UK business would also represent success, however due to current underreporting and the lack of a true baseline, measurement will not necessarily be possible.

56. Interventions by Law Enforcement to takedown and disrupt criminal actors, such as the intervention against LockBit are illustrative of what the legislative proposals intend to support, disrupting the cyber crime business model. Post intervention, there was no income generated for many LockBit affiliates, despite the significant outlay required, reducing criminal incentive to attack.

57. Increased reporting will provide the government with greater knowledge of ransomware payments which will give law enforcement and intelligence partners the opportunity to intervene and support victims.

58. Greater oversight and information on criminal actors from increased reporting would also support law enforcement in the sanctioning of criminal actors, further disrupting the criminal business model.

4. Description of proposed intervention options and explanation of the logical change process whereby this achieves SMART objectives

59. The overall motivation for intervention is to reduce crime and associated harms to UK businesses, reducing the threat of ransomware attacks by making the UK a less attractive target to ransomware criminals. This will be achieved through three main strategic objectives:

- Reduce the amount of money flowing to ransomware criminals from the UK, thereby deterring criminals from attacking UK organisations.
- Increase the ability of operational agencies to disrupt and investigate ransomware actors by increasing our intelligence around the ransomware payment landscape.
- Enhance the government's understanding of the threats in this area to inform future interventions, including through cooperation at international level.

60. The shortlisted options for consultation are as follows, options are explained in detail in Section 6: Description of shortlisted policy options carried forward:

Option 0: Do Nothing.

Option 1: A complete ban on ransomware payments.

Option 2: A targeted ban on ransomware payments for regulated CNI and the public sector.

Option 3: A ransomware payments prevention regime for all ransomware payments.

Option 4: Mandatory reporting of a payment prior to the transaction (sector specific or economy wide).

Option 5: A mandatory ransomware incident reporting regime for all sectors.

Option 6: Mandatory reporting of ransomware incidents for specific sectors.

61. A reduction in repeat attacks on victims either by the same criminal or ransomware strand will allow the Home Office to measure success as an indicator of the UK's resilience, either to be able to: recover fully from the first attack and block subsequent attacks; or deter repeat attacks.

62. A reduction in payments to ransomware actors from UK business would also represent success, however due to current underreporting and the lack of a true baseline, measurement will not necessarily be possible.

63. The proposed legislative options aim to reduce the risk of harm from ransomware to the UK, a logic model is presented below:

- **Outcome 1**: Reduce criminal intent, through undermining the ransomware business model.

  Reducing the amount of money flowing to ransomware criminals will undermine the ransomware business model, making the UK a less attractive target to criminals.

- **Outcome 2**: Reduce criminal capability, through bolstering UK law enforcement ability to disrupt and investigate ransomware criminals.

  The government will be able to increase operational partners ability to disrupt and investigate ransomware actors by increasing the government's visibility and knowledge of the ransomware payment landscape.

- **Outcome 3**: Reduce vulnerability, through improving resilience.

  The government will use improved reporting to identify, track and mitigate vulnerabilities, through increased understanding of the threat landscape.

- **Outcome 4**: Reduce impact, through expanding preparedness.

  The government will use improved reporting to increase understanding of the threat landscape to inform future interventions.

5. Summary of long-list and alternatives

Discarded alternatives from the long-list

Non-Regulatory options

64. Non-regulatory options have been explored fully and deemed insufficient due the need to adequately mitigate the harm that ransomware and emerging technologies pose to the UK. New policies will be part of a holistic approach that will not replace any non-regulatory interventions already in place but will be used to elevate and future proof the UK response to this evolving cyber harm.

65. Existing non-regulatory options include HMG's existing policy position that no HMT funds can be used to make ransomware payments; NCSC guidance designed to help victims: mitigate against attacks, create resilient cloud backups, recover infected devices, recover hacked accounts, and negotiate the issue of payment of ransoms.[50] The ICO provide ransomware and data protection compliance checklist to reduce vulnerability for business, covering: governance, asset identification, access controls, vulnerability management, staff education, detection, and incident response.[51]

66. Over time the government has observed that most criminal and hostile actors that use ransomware are based in jurisdictions that the UK has limited relationships with. The UK has very limited levers, which impedes the ability of operational partners to sanction, seize, and convict these actors, and return funds back to victims.

67. The main mitigation against ransomware is to change victim behaviour. To mobilise this change swiftly and in a way that will have lasting impact to the UK. Internationally setting the tone that "the UK does not pay", deterring future and repeat offences requires a shift in how the government views compliance in a digital age and digital Britain. This requires the Home Office to go beyond the non-regulatory measures currently in place and implement legislation.

[50] Ransomware - NCSC.GOV.UK, https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=ransomware&sort=date%2Bdesc&articleType=guidance

[51] Ransomware and data protection compliance | ICO, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/a-guide-to-data-security/ransomware-and-data-protection-compliance/

6. Description of shortlisted policy options carried forward

Option 0: 'Do nothing'

68. Under the 'Do nothing' option, money will continue to flow from UK businesses to ransomware criminals. There would be no improvement in visibility or knowledge of the ransomware payment and threat landscape; this would continue to hamper operational partners ability to disrupt and investigate ransomware actors, and the governments' ability to make targeted policy interventions.
69. Stakeholders agree that the government must act, that the status quo is not sustainable in protecting the UK, and there is a clear acknowledgment that the implementation of any approach will be difficult and novel.
70. **Options relating to strategic objective 1**: Reduce the amount of money flowing to ransomware criminals from the UK, thereby deterring criminals from attacking UK organisations.

Option 1: A complete ban on ransomware payments.

71. A ban on payments from all UK-based individuals, UK businesses or businesses operating in the UK to ransomware criminal actors for de-encryption of data and systems, to supress leaking of exfiltrated data, or for any other reason.
72. The Home Office has undertaken significant external stakeholder engagement and has found that there is limited industry support for a complete ban on payments. There is consensus that in some circumstances a payment is the best option for a victim, and they should be able to pay as a last resort.

Option 2: A targeted ban on ransomware payments for regulated CNI and the public sector.

73. A ban on payments for the public sector and regulated CNI sectors.
74. The Home Office is considering the scope of the public and CNI sectors to be covered by the proposed ban. The Home Office currently proposes that the ransomware payment ban would cover the public and CNI sectors:
    - The public sector, including: all local authorities, schools, and the wider public sector including the health sector.
    - The CNI sector: CNI owners and operators (in sectors defined by the National Protective Security Authority, subject to regulation/competent authorities). The Home Office will consult with CNI Departments and wider industry. It may be prudent to initially cover only a limited number of CNI entities and expand the remit of the legislation over time. This would allow time to bring in relevant support and mitigations. The Home Office is aware of the CNI supply chain and its size, and is seeking views through the consultation as to whether essential suppliers to the CNI sectors should be covered by the proposed ban.
75. This intervention would be accompanied by clear guidance on payments addressed to the wider economy, aiming to change behaviours around data suppression payments.

76. Victims could attempt to find alternative ways to pay. However, as it would be unlawful for organisations covered by the proposed ban to make a payment, the Home Office believes that most reputable cryptocurrency brokers would not process such transactions. The government would produce specific guidance and communications to cryptocurrency brokers.

77. It is assumed that due to the nature of the CNI and public sectors that this option will not have a disproportionate impact on micro, small, and medium sized businesses (SMBs). The consultation will test the scope of the ban and whether CNI supply chains should be included. More SMBs would be captured by this option if the supply chain was included, which will be taken into account when deciding whether to include the supply chain in the scope. The Home Office will take consultation responses into account to ensure all effects and possible mitigations are considered.

78. There is the risk that by including CNI and the public sector in the ban, ransomware attacks will be displaced onto the wider economy. However, due to the opportunistic nature of ransomware attacks, this is viewed to be low-risk. We are exploring mitigations for this, and this will be a metric in our monitoring and evaluation plan.

79. **Options relating to strategic objective 2**: Increase the ability of operational agencies to disrupt and investigate ransomware actors by increasing our intelligence around the ransomware payment landscape.

Option 3: Payment prevention regime for all other ransomware payments.

80. Whilst payments would remain legal, the government could criminalise payments not reported into and reviewed by the government ahead of time. This would increase the government's understanding of payments and could prevent a payment when appropriate, drawing on the Terrorist Financing model.[52]

81. The Home Office believes that payment prevention could lead to changes in victim behaviour, potentially encouraging additional decisions around making a payment, such as exploring backups and other resilience measures. Engagement with the government implies that organisations may take the view that there is a high bar to meet if they should decide to facilitate a ransomware payment.

82. There are two types of ransomware payments: a transactional payment for a decryption key, and an extortion-type payment for data suppression. The payment prevention regime, underpinned by comms and guidance, could reduce the levels of data suppression payments, supporting the industry consensus that the government should do so. We are exploring through the consultation whether the regime should apply to all potential victims (including smaller businesses, charities and members of the public) or whether it should be threshold-based (e.g. size of the organisation, amount of ransom demanded).

83. The reporting timeframe is being explored through the consultation to ensure it is appropriate and does not overburden victims. Ransomware groups are agile in adapting demands to the legislative environment (for example, noting the size of ICO fines when making demands). It can be assumed criminals will adapt their demands to match the timeframe within which reports must be made to the government.

[52] Countering Terrorist Financing - GOV.UK (www.gov.uk), https://www.gov.uk/government/publications/countering-terrorist-financing/countering-terrorist-financing

84. There is the potential to force payments underground or for businesses to use unreputable brokers. Reputable brokers would still likely avoid such business. The government will introduce specific guidance and work with industry and international counterparts, particularly the US, for consistent messaging.

85. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. The Home Office aims to mitigate possible impacts to SMBs by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects and possible mitigations are considered.

Option 4: Mandatory reporting of a payment prior to the transaction

86. This measure would take the form of an informing mechanism rather than a review mechanism akin to the kidnap and ransom model.[53] Victims who are intending to make a payment to a ransomware criminal would be required to report their intention into government. This would not be accompanied by any review mechanism.

87. Any level of mandatory reporting will increase the government's awareness and understanding of the threat landscape. Mandatory reporting alone (without complementary levers and/or significant enforcement measures) will not substantively change the status quo.

88. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. However, as Option 4 will require less business capacity to complete than Option 3, impacts are assumed to be smaller. The Home Office aims to mitigate possible impacts to SMBs by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects and possible mitigations are considered.

89. **Options relating to strategic objective 3:** Enhance the government's understanding of the threats in this area to inform future interventions, including through cooperation at international level.

Option 5: A mandatory reporting regime for all sectors.

90. Victims of a ransomware attack should report the incident to a suitable reporting mechanism within a mandatory timeframe.

91. Our international counterparts (Australia, the USA, and others) have introduced mandatory reporting mechanisms with varying successes. The Home Office would attempt to replicate the data required, whilst also incorporating the needs of policy and operational partners.

92. When introducing a mandatory reporting regime, The Home Office would clearly articulate:

- Why the government wants the data,
- Where the government will store the data, how, and if the data will be shared,
- What the government will do with the data,

[53] Fact sheet - Kidnap and ransom (publishing.service.gov.uk), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/540539/CTS_Bill_-_Factsheet_9_-_Kidnap_and_Ransom.pdf

- Manage expectations around the low likelihood of securing domestic criminal justice outcomes and arrests.
- What support the government will provide on receipt of a report (including, but not limited to, improving the victim journey and interaction with the reporting mechanism).

93. Any reporting mechanism risks non-compliance. This effect has not been reported by new demands in the recent US, Australian, or French governmental regimes. A mandatory regime could raise compliance from current levels.

94. A suitable mechanism must require sufficient incident detail but avoid being onerous. The government would mandate certain essential information and provide the opportunity for further details on a voluntary basis, to minimise negative impacts.

95. There is risk of victim fatigue, there are already several mandatory reporting requirements, including to the ICO for data protection breaches, and particularly for CNI sectors. The government must ensure that new mechanism aligns with these and demonstrate their added value.

96. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. The Home Office aims to mitigate possible impacts to SMBs by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects and possible mitigations are considered.

Option 6: Mandatory reporting of ransomware incidents for specific sectors

97. Option 6 represents a less stringent version of Option 5, only targeted at specific sectors (for example, CNI if a ban is not introduced). Or, we would limit who would be covered via a threshold-based approach, which could explore organisation size or turnover.

98. The Home Office is consulting on the best measures for encouraging compliance with this regime, such as whether to impose criminal and/or civil penalties for non-compliance, especially where a payment is made after the victim has been told it has to be blocked, and whether this regime and any accompanying compliance measures should apply to all potential victims – including smaller businesses, charities and members of the public – or whether a higher threshold should be set for the size of the organisation and/or the amount of the ransom demanded.

99. This would give a limited view of the threat and may be viewed as disproportionate and unviable due to the changes required for limited data insights.

100. There is a risk to sector specific reporting if ransomware payments are forced underground, the government could see cyber attackers solely targeting sectors or areas of the UK economy that have limited or no reporting contributing to an inaccurate intelligence picture and potentially putting some sectors at risk unnecessarily.

101. It is assumed that due to the nature of the CNI that this option will not have a disproportionate impact on SMBs. The Home Office will take consultation responses into account to ensure all effects and possible mitigations are considered.

7. Monitoring and evaluation

102. Any option taken into legislation would be monitored against key success metrics, Home Office and wider government strategy. Such options would be subject to a post implementation review (PIR) as part of the Home Office's overall evaluation strategy. The nature of further evaluation undertaken will be assessed based on the feasibility and proportionality of wider process or impact evaluation.

103. The evidence base around ransomware is currently limited due to underreporting. Data gathered through intervention, or consultation, will be used to better monitor the success of law enforcement activities and outcomes.

104. Any measure introduced to improve reporting would allow the government to better monitor and evaluate the impact of the legislation due to greater knowledge of the ransom payment landscape and ransomware criminal business model.

105. The impact of intervention on UK businesses will be monitored and evaluated through evidence from improved reporting to measure success and search for any unintended consequences.

8. Minimising administrative and compliance costs

106. To minimise administrative burdens for Options 1 and 2, relating to bans on ransomware payments, the Home Office will make every effort post consultation to incorporate findings to minimise the time taken for familiarisation for businesses to new laws with simple, complete, and concise guidance. The Home Office will build on the experience, successes, and any current and future evaluation of similar interventions such as sanctions to ensure the process has the lowest possible time cost to impacted businesses.

107. To minimise administrative burdens for Options 3 and 4, relating to payment prevention, the Home Office will make every effort post consultation to incorporate findings to minimise the time taken for familiarisation for businesses to new laws with simple, complete, and concise guidance. The Home Office will incorporate all current and future best practice to ensure engagement requirements are as clear as possible, reducing the impact to businesses as much as is possible.

108. To minimise administrative burdens for Options 5 and 6, relating to reporting, the Home Office will make every effort post consultation to incorporate findings to minimise the time taken for familiarisation for businesses to new laws. The Home Office will incorporate all current and future best practice to ensure reporting requirements are as clear as possible, reducing the impact to businesses as much as is possible.

Declaration

Department: Home Office

Contact details for enquiries:

ransomwareconsultation@homeoffice.gov.uk

Minister responsible: Dan Jarvis MBE MP, Minister for Security

I have read the Consultation Options Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed:

Date: 14/01/2025

Summary: Analysis and evidence

Price base year: 24/25

PV base year: 2024

This table may be reformatted provided the side-by-side comparison of options is retained	**0. Do Nothing (baseline)**	**1. Shortlist Option 1:** A complete ban on ransomware payments	**2. Shortlist Option 2:** A targeted ban on ransomware payments for regulated CNI and the public sector	**3. Shortlist Option 3:** A ransomware payments prevention regime for all other ransomware payments.	**4. Shortlist Option 4:** Mandatory reporting of a payment prior to the transaction
Net present social value and list of central value of monetised costs (with brief description, including ranges, of individual costs and benefits)	…	-£5.3m (Public Sector running costs: £4.3m; Private Familiarisation Costs: £0.97m; Public Familiarisation Costs: £7,900 Monetised Benefits: None)	-£2.1m (Public Sector running costs: £2.1m; Private Familiarisation Costs: £10,000; Public Familiarisation Costs: £7,900. Monetised Benefits: None)	-£18.3m (Public Sector running costs: £17.3m; Private Familiarisation Costs: £0.97m; Public Familiarisation Costs: None. Monetised Benefits: None)	-£9.5m (Public Sector running costs: £8.4m; Private Familiarisation Costs: £0.97m; Public Familiarisation Costs: None. Monetised Benefits: None)
Public sector financial costs (with brief description, including ranges)	…	Public sector setup costs: Not monetised (see cell below). Public sector running cost: (l: £1.3m, c: £4.3m, h: £5.4m)	Public sector setup costs: Not monetised (see cell below). Public sector running costs: (l: £1.0m, c: £2.1m, h: £3.2m)	Public sector setup costs: Not monetised (see cell below). Public sector running costs: (l: £5.2m, c: £17.3m, h: £21.6m)	Public sector setup costs: Not monetised (see cell below). Public sector running costs: (l: £3.9m, c: £8.4m, h: £13.0m)
Significant un-quantified benefits and costs (description, with scale where possible)	…	**Public Sector Monitoring and Enforcement Costs:** It is anticipated that there will be some basic costs to setup an effective monitoring and enforcement	**Public Sector Monitoring and Enforcement Costs:** It is anticipated that there will be some basic costs to setup an effective monitoring and	**Public Sector cost of creating the capability to monitor and enforce the regime:** There will be costs to setup an review regime which responds	**Public Sector setup cost:** Cost of creating the capability to monitor and enforce reporting. There will be costs to setup a mechanism

		regime to oversee the individuals and organisations within the scope of the ban. **Benefits:** It is expected that the number of ransomware payments made will be dramatically lower, and this significantly reduces incentive to attack for financially motivated attackers over the long term. There are also benefits to organisations from a lower level of ransomware attacks such as lower ransomware insurance costs.	enforcement regime to oversee the organisations within the scope of the ban. **Benefits:** As in Option 1, but only for CNI and the public sector.	sufficiently quickly and can guide businesses through the process. **Benefits:** It is expected that an increased knowledge of payments and interactions with attackers as a direct result of the review regime will improve the government's intervention.	which can guide businesses through the process. **Benefits:** Any level of mandatory reporting will increase the government's awareness and understanding of the threat landscape, however this option is largely complimentary to other measures as in isolation there are no identified direct benefits.
Key risks (and risk costs, and optimism bias, where relevant)		Since this OA is still at consultation stage the cost estimates are a guide rather than full calculation. This is because both the chosen options and the precise extent and design of the options will be decided after taking on board feedback from the consultation. At that point a more complete and accurate costing with full risks and optimism bias can be applied.			

This table may be reformatted provided the side-by-side comparison of options is retained	**5. Shortlist Option 5:** A mandatory reporting regime for all sectors	**6. Shortlist Option 6:** Mandatory reporting of ransomware incidents for specific sectors
Net present social value and list of central value of monetised costs (with brief description, including ranges, of individual costs and benefits)	-£5.6m (Public Sector running costs: £4.3m; Private Familiarisation Costs: £0.97m; Public Familiarisation Costs: £7,900. Monetised Benefits: None)	-£2.1m (Public Sector running costs: £2.1m; Private Familiarisation Costs: £10,000; Public Familiarisation Costs: £7,900. Monetised Benefits: None)
Public sector financial costs (with brief description, including ranges)	Public sector setup costs: Not monetised (see cell below). Public sector running costs : (l: £1.3m, c: £4.3m, h: £5.4m)	Public sector setup costs: Not monetised (see cell below). Public sector running costs: (l: £1.0m, c: £2.1m, h: £3.2m)
Significant un-quantified benefits and costs (description, with scale where possible)	**Public sector setup cost:** The government will need to allocate initial additional resources to the reporting mechanism which can advise, accept and monitor reports. Any additional support that the government provides on receipt of a report will need to be setup. **Benefits:** Data received from the reports will improve HMGs knowledge and understanding of the threat landscape.	**Public sector setup cost:** The government will need to allocate initial additional resources to the reporting mechanism which can advise, accept and monitor reports. Any additional support that the government provides on receipt of a report will need to be setup. **Benefits:** As in Option 5, but limited to CNI and the public sector, dependent on threshold.
Key risks (and risk costs, and optimism bias, where relevant)	Since this OA is still at consultation stage the cost estimates are a guide rather than full calculation. This is because both the chosen options and the precise extent and design of the options will be decided after taking on board feedback from the consultation. At that point a more complete and accurate costing with full risks and optimism bias can be applied.	

Annex

Evidence Base

Appraisal

General assumptions and data

1. The general assumptions used in this OA are as follows:
    - The appraisal period for measuring the impacts is 10 years, starting in 2024/25.
    - A 3.5 per cent annual social discount rate is used, as per HMT Green Book guidance.[54]
    - Annual costs and benefits are presented in 2024/25 prices, when necessary, prices are deflated into 2024/25 prices using HMT GDP deflators[55]
    - All costs and benefits are relative to the **Option 0: 'Do Nothing'.**

Summary of Costs

Familiarisation Costs

2. Familiarisation costs are applied to all options requiring organisations to read new guidance.
3. Three different familiarisation cost estimates are provided:
    - Familiarisation costs that apply to all businesses, Table 2.
    - Familiarisation costs that apply only to CNI, Table 3.
    - Familiarisation costs that apply only to the public sector, Table 4.
4. It is assumed that:
    - Approximately 16 per cent of UK organisations read 1000 words on a screen to become familiar with the new guidance, proxy estimate for proportion of businesses who read taken from proportion of businesses aware of government guidance, initiatives or communication campaigns, CSBS, 2024.[56]
    - The likelihood of reading increases as the size of the organisation by number of employees increases.
    - Between one and eight people in each firm will need to become familiar with the new guidance across the estimates and depending on organisation size.

[54] https://www.gov.uk/government/publications/the-green-book-appraisal-and-evaluation-in-central-government/the-green-book-2020
[55] GDP deflators at market prices, and money GDP - GOV.UK (www.gov.uk) https://www.gov.uk/government/collections/gdp-deflators-at-market-prices-and-money-gdp
[56] Cyber security breaches survey 2024 - GOV.UK (www.gov.uk), https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024#chapter-2-awareness-and-attitudes

5. It is anticipated that relevant staff in reading organisations would have to familiarise themselves with the changes and read the guidance provided by the government. For smaller organisations, it is expected that there will be a lower rate of familiarisation through permanent employees, and that instead this cost would be fed through the cost of employing cybersecurity experts who would be familiar with the guidance.

6. Typically, time will be spent building an understanding of what the legislation means and its relationship with existing policies. Depending on the chosen options, some measures may affect only CNI businesses and the public sector, or all organisations.

7. For all firms, time has been valued using data from the Annual Survey of Hours and Earnings (ASHE) 2022, Table 14.5a.[57] The analysis uses a median wage figure for cyber security professionals (Standard Occupational Classification (SOC) code 2135) of £22.62 per hour, which is then uplifted by the non-wage share of costs of 22 per cent to reflect the marginal product of labour [58] and adjusted for inflation using 2024/25 prices.

8. The values used to estimate the familiarisation costs are presented in Tables 2, 3 and 4 and given as:

Number of firms x number of readers in each firm x average familiarisation time x (median cyber security professionals wage x non-wage uplift of 22%)

Private sector familiarisation

Table 2, Familiarisation costs to all private organisations in year 1 only, FY 2024/25.

Estimate	Number of firms	No. readers per firm	No. words to read	Reading speed (wpm)	Average time (hrs)	Cost per hour (£)	Cost to business (£m)
Low	387,802	1.06	1,000	700	0.02	29.59	**0.2**
Central	408,152	1.32	1,000	300	0.08	29.59	**1.0**
High	795,954	2.39	1,000	200	0.15	29.59	**3.1**

Source: ONS, UK Business, activity, size and location, 2024, ASHE 2020 Table 14.5a., Home Office Internal Analysis.

9. Private sector familiarisation costs for all private organisations are estimated to lie in a range of **£0.2 million to £3.1 million**, with a central estimate of **£1.0 million**, in year one only.

[57] ONS Earnings and hours worked, occupation by four-digit SOC: ASHE Table 14, https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/earningsandworkinghours/datasets/occupation4digitsoc2010ashetable14

[58] Non-wage cost is 17.9 per cent (from Eurostat), take 18/(100-18) = 18/82 = 22 per cent and uplift by this amount. https://ec.europa.eu/eurostat/databrowser/view/LC_LCI_LEV__custom_2052124/default/table?lang=en.

Table 3, Familiarisation costs to CNI organisations in year 1 only, FY 2024/25.

Estimate	Number of firms	No. readers per firm	No. words to read	Reading speed (wpm)	Average time (hrs)	Cost per hour (£)	Cost to business (£'000)
Low	3,878	1.51	1,000	700	0.02	29.59	**2.3**
Central	4,212	2.31	1,000	300	0.08	29.59	**10.0**
High	9,955	3.81	1,000	200	0.15	29.59	**38.3**

Source: ONS, UK Business, activity, size and location, 2024, ASHE 2020 Table 14.5a., Home Office Internal Analysis.

10. Familiarisation costs for CNI organisations only are estimated to lie in a range of **£2,300 to £38,300**, with a central estimate of **£10,000**, in year one only.

Public sector familiarisation

Table 4, Familiarisation costs to public sector organisations in year one only, FY 2024/25.

Estimate	Number of firms	No. readers per firm	No. words to read	Reading speed (wpm)	Average time (hrs)	Cost per hour (£)	Cost to business (£'000)
Low	2,393	1.51	1,000	700	0.02	29.59	**1.4**
Central	3,355	2.31	1,000	300	0.08	29.59	**7.9**
High	5,748	3.81	1,000	200	0.15	29.59	**22.1**

Source: ONS, UK Business, activity, size and location, 2024, ASHE 2020 Table 14.5a., Home Office Internal Analysis.

11. Familiarisation costs for public sector organisations only are estimated to lie in a range of **£14,000 to £22,100**, with a central estimate of **£7,900**, in year one only.

Compliance

12. The affected organisations under each option could incur costs to ensure compliance with the policy. In addition to familiarisation, it is possible that the organisations may need to redesign their cyber policies, which may involve staff with higher wage costs (for example, senior management). It is also expected that there will be ongoing costs to organisations for trained employees to ensure compliance post familiarisation.

13. However, firms already have compliance responsibilities such as complying with sanctions. Synergies are expected due to the familiarity of some organisations with existing reporting and compliance processes which will have similarities with the ransomware reporting and compliance regime.

14. These costs have not been quantified at this time due to insufficient data, which the Home Office is looking to gather during the consultation.

Public Sector Monitoring and Enforcement Setup Costs

15. It is anticipated that there will be some significant costs to setup an effective monitoring and enforcement regime to oversee the organisations within the scope of the chosen options. This will likely centre around staffing and an IT system similar to the Enhanced Cyber Reporting Service (ECRS)[59]. Those working in monitoring and enforcement will need to be trained. These setup costs are not monetised at this stage since the department is still consulting on options.

16. Public servants working in this area will need to read and understand how the partial ban will work. There will be a small time-cost for reading and processing any implications.

17. This reading cost is expected to be negligible, but through the consultation a final option will be decided and any documentation to be read by public servants will be written. This cost may be updated following consultation responses to include a small awareness time cost.

The extent of CNI and public organisations which would be affected in Option 2 (partial ban of ransomware payments) and options 4 and 6.

18. Public Sector: The number of local authorities, schools, and the wider public sector including the health sector. This is approximately 12,485[60].

19. In the UK, there are 13 Critical National Infrastructure Sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, government, Health, Space, Transport and Water.

20. The number of CNI organisations that are proposed to be included in the ban includes CNI owners and operators (in sectors defined by the National Protective Security Authority, subject to regulation/competent authorities). This excludes the CNI supply chain. Since there is not a strict definition of what constitutes a CNI organisation, we approximate this number as one per cent of all private organisations. This is 26,668[61].

Additional recovery costs

21. There is the potential for additional recovery costs to all organisations or CNI or the public sector due to banning of ransom payments in Options 1 and 2.

22. There is mixed evidence around the additional recovery costs that organisations incur from not paying a ransom, compared to paying a ransom, when subject to a ransomware attack. The consultation aims to gather more evidence around this subject.

Administration costs related to information submissions

[59] The National Fraud Intelligence Bureau's dedicated 24-hour cybercrime reporting and triage service for businesses.

[60] Sum of central government, public corporation and local authority. Table 14, UK Business, activity, size and location, 2023 (ons.gov.uk). https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/datasets/ukbusinessactivitysizeandlocation

[61] Table 14, UK Business, activity, size and location, 2023 (ons.gov.uk). https://www.ons.gov.uk/businessindustryandtrade/business/activitysizeandlocation/datasets/ukbusinessactivitysizeandlocation

23. There will be a cost burden imposed on in-scope organisations due to reporting requirements in Options 3, 4, 5 and 6. It is envisaged that organisations will need to share the required information to a third-party platform in a similar way to the submission of Suspicious Activity Reports (SARs), which are used as a proxy factor for information submission costs[62].

24. The number of SARs submissions between 2024/25 and 2031/32 is estimated to be between 41,000 and 207,000 with a central estimate of 95,000. The proxy factor is calculated by taking the multiple between the low and central submissions $\frac{95,000}{41,000}$=2.32, and between the central and high submissions $\frac{207,000}{95,000}$=2.18.

25. It is estimated that submitting information about one customer to the third-party platform would take 30, 45 and 60 minutes (in Low, Central and High cases).

26. For all organisations, time has been valued using data from the Annual Survey of Hours and Earnings (ASHE) 2022, Table 14.5a. The analysis uses a median wage figure for administrative occupations: finance, SOC code 412, of £13.03 per hour, which is then uplifted by the non-wage share of costs of 22 per cent to reflect the marginal product of labour.

27. The number of submissions is calculated differently for the public and private sector, since public sector organisations are included in all options, unlike the private sector where only CNI is always included, creating a different cost for each category, as follows.

Private Sector

28. Firstly, Options 3 and 4 are estimated in table 6. The central (number of information submissions) figure is based on the five-year average of the number of ransomware incidents reported to the ICO from 2019 to 2023, after removing public sector reports which is assumed to be 0.5 per cent. The low and high figures are then reduced and uplifted respectively by the same factor as for SARs submissions.

29. Secondly, Option 5 is estimated in table 7. Each estimate takes the 5-year average of ICO ransomware incidents and divides them by an assumed ransom payment rate (table 5).

Table 5, Summary of the estimated Ransomware payment rates

	Ransom Payment Rate (per cent)	Source
Low	11	Trend Micro[63]
Central	22	Home Office Calculations
High	33	NCA

[62] As set out in paras 14 & 15 on page 6 and para 54 & table 5 on page 16 of the Information sharing between regulated entities Impact Assessment.
https://assets.publishing.service.gov.uk/media/63d270a3e90e071ba44851f9/_f__Information_Sharing_IA_Jan_2023_-_signed.pdf

[63] This figure is for Europe. Page 7, What Decision-Makers Need to Know About Ransomware Risk (trendmicro.com).
https://documents.trendmicro.com/assets/white_papers/wp-what-decision-makers-need-to-know-about-ransomware-risk.pdf#page=7

30. To account for underreporting to the ICO, the ransom payment rate is used as a proxy. The low estimate for the number of information submissions is calculated by dividing the low ICO estimate of ransomware attacks by the high (33 per cent) ransom payment rate, which is an NCA estimate of the number of UK victims which engaged with criminals[64]. The high estimate takes the high ICO estimate, divided by the low estimate of the ransom payment rate, (11 per cent). The central value takes central ICO estimate and the midpoint ransom payment rate (22 per cent).

31. Lastly, Option 6 is estimated in table 8. This takes the number of information submissions for Option 5 and then multiplies the low, central, and high by 0.01 to account for the smaller number of organisations in scope within Option 6 (assumed to be CNI organisations only).

32. The values used and the estimated private administration costs of information submissions are presented in Tables 5 to 7 and are given as:

Number of information submissions (see Tables 5 to 7) x average time to submit to the platform (see Tables 5 to 7) x (median administrative occupations: finance wage x non-wage uplift of 22%)

Table 6, Option 3 and 4, Private Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£m)
Low	283	0.5	15.87	**0.02**
Central	656	0.75	15.87	**0.07**
High	1,430	1	15.87	**0.21**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

33. Total administration costs lie in a range of **£0.02** to **£0.21 million**, with a central estimate of **£0.07 million** (PV over 10 years).

Table 7, Option 5, Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£m)
Low	858	0.5	15.87	**0.06**
Central	2,984	0.75	15.87	**0.33**
High	13,002	1	15.87	**1.9**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

[64] Figure for engagement with LockBit specifically.

34. Total administration costs lie in a range of **£0.06** to **£1.9 million**, with a central estimate of **£0.33 million** (PV over 10 years).

Table 8, Option 6, Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£'000)
Low	9	0.5	15.87	**0.63**
Central	30	0.75	15.87	**3.3**
High	130	1	15.87	**19.1**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

35. Total administration costs lie in a range of **£630** to **£19,100**, with a central estimate of **£3,300** (PV over 10 years).

Public Sector

36. Options 3 and 4 are assumed to incur zero public sector submission costs because we assume that public sector organisations cannot pay a ransom. This is due to the government's current position, where no central government funds can be used to pay a ransom.

37. Option 5 is estimated in table 9. The low figure is based on five-year average of the number of ransomware incidents reported to the ICO by central and local government and regulators. The central estimate includes in addition reports under health and justice, which is then multiplied by the same SARs factor as in Option 3 and 4 to create the high estimate.

38. Option 6 costs are identical to Option 5 here since we are only considering public sector costs.

39. The values used and the estimated public administration costs of information submissions are presented in tables 8 and 9.

Table 9, Option 5 and 6 Public Sector Administration costs for information submissions over 10 years, FY 2024/25

Estimate	Number of information submissions (yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£'000)
Low	40	0.5	15.87	**3.0**
Central	86	0.75	15.87	**9.4**
High	187	1	15.87	**27.4**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

40. Total public sector administration costs lie in a range of **£3,000** to **£27,400**, with a central estimate of **£9,400** (PV over 10 years).

Cost to international businesses of overlap

41. There may be costs to international businesses of having overlap costs from regulation differing by country. For example, if the precise requirements of the UK regime differs from that of Australia or the US, there may be additional costs to business compared to a more similar option. This is particularly relevant for Option 5 because some international counterparts have introduced mandatory reporting mechanisms already, whereas bans on ransom payments are more novel.

Public Sector Running costs

42. Once set up, each option will incur operational costs for the public sector, comprising staffing to monitor and advise organisations, and the maintenance of any IT. This will vary depending on the decided scope of the options post consultation, and some of the costs of the options will be shared if they are chosen in combination, for example if Option 2 and Option 4 are chosen, there is likely to be partial overlap costs. This means that the cost of choosing multiple options is not necessarily cumulative.

43. The cost of the ECRS (a 24-hour cybercrime reporting and triage service for business launched by the National Fraud Intelligence Bureau in September 2022) is used as an approximation for the operational public sector cost. The FY 2023 to 2024 total cost for ECRS was £1.7 million. The present value cost over the 10-year period of this OA is £15.2 million. It is assumed that the public sector running cost of Options 1 to 6 will be similar to the ECRS costs, although a more precise estimate will be made following the consultation based on the chosen options.

44. An approximate public sector running cost has been assigned to each option, however these costs should be interpreted as approximate and ordinal in nature, rather than a precise bottom-up value.

Which assumption cost apply to which OA option.

45. Many of the costs considered thus far appear in multiple options. Table 10 is included to provide a simple guide for which costs apply to each option, although they are also all listed below in the cost and benefits section.

Table 10, Summary of recurring costs relevant to each OA option. Green fill and text indicates that the cost applies (£ million)

Option	**0**	**1**	**2**	**3**	**4**	**5**	**6**
Cost (£m)							
Familiarisation Costs		1.0	0.02	1.0	1.0	1.0	0.02
Administration Costs				0.1	0.1	0.3	0.01
Additional recovery costs		Not Monetised					
Compliance Costs		Not Monetised					
Public sector running costs		4.3	2.1	17.3	8.4	4.3	2.1

Source: Home Office Internal Analysis

Summary Of Benefits

46. No benefits have been monetised due to the variability and uncertainty around cyber criminals' behaviour. A significant proportion of the benefits are in fact informational as the various reporting requirements will improve future government interventions. These factors, along with the direct impacts of banning payments are discussed further under each option below. The potential monetary impact of the options is explored through a sensitivity analysis immediately after the cost and benefits of options section.

47. Firms will benefit from the results of increased compliance and improved cyber hygiene through reduced risk of attack and associated harms.

48. These benefits have not been quantified at this time due to insufficient data, which the Home Office is looking to gather during the consultation.

49. Sensitivity analysis has been performed using case studies from previous and possible future ransomware attacks. This includes estimates from the Department of Health and Social Care costing of the WannaCry cyber-attack to the NHS, and a hypothetical ransomware attack on the South East electricity grid based on a stress test report by the Cambridge Centre for Risk Studies. The analysis investigates the benefit from harms avoided derived from either lowering the impact of such an attack or the probability of a similar attack happening in the future, as well as a breakeven test.

COST AND BENEFITS OF OPTIONS

Option 0: Do Nothing

50. Cost and benefits, when quantified or monetised are compared to the 'Do nothing' Option.

Option 1: A complete ban on ransomware payments.

51. A ban on payments from all UK businesses or businesses operating in the UK to ransomware criminals for de-encryption of data and systems, to supress leaking of exfiltrated data or for any other reason.

COSTS

Set-up Costs

Private Sector Costs

Private Sector Familiarisation Costs

52. The government anticipates that relevant staff in reading organisations would have to familiarise themselves with the changes and read relevant information provided by the government.

53. For smaller organisations, the government expects that there will be a lower rate of familiarisation through permanent employees, and that rather this cost would be fed through the cost of employing cybersecurity experts who would be much more likely to be familiar with the guidance. These costs are set out in Table 2 above.

Public Sector Costs

Familiarisation costs to public sector organisations to comply with the regime

54. The government anticipates that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information provided by the government such as the guidance. These costs are set out in Table 4 above.

Public Sector Monitoring and Enforcement Costs

55. The government anticipates that there will be some basic costs to setup an effective monitoring and enforcement regime to oversee the organisations within the scope of the partial ban. This will likely centre around staffing and an IT system like ECRS. Those working in monitoring and enforcement will need to be trained.

56. Public servants working in this area will need to read and understand how the partial ban will work. There will be a small-time cost for reading and processing any implications. This cost is expected to be negligible.

Ongoing Costs

Private Sector Costs

Ongoing costs to all private organisations of complying

57. There will be some ongoing training costs and staff time costs for private organisations to interact with the government based on new regulations and other new staff training.

Additional recovery costs

58. It is likely that until attackers learn that all UK organisations won't pay a ransom, they will continue attacks. If payments are banned, then recovery from ransomware attack for chosen businesses and public bodies will be more costly than the ‘Do nothing’ option. The additional costs from this policy would predominately be for private organisations since local authorities are already not allowed to use central government funds to pay ransoms.

Risk of adverse incentives

59. There is a risk of adverse incentives, victims could reduce engagement or go underground. However, it would be unlawful to make a payment, so most reputable crypto brokers would not process such transactions. It may prove difficult to find alternative routes to pay. The government would produce specific guidance and comms to crypto brokers.

Public Sector Costs

Cost of running the capability to monitor and enforce the ban

60. Once the monitoring and enforcement regime is set up there will be operational costs, this includes costs for staffing to monitor and advise organisations, and the maintenance of any IT. A proxy for this cost is set out above in the appraisal cost summary section under the heading 'Public Sector Running costs'.

61. Total public sector running costs lie in a range of **£1.3** to **£5.4 million**, with a central estimate of **£4.3 million** (PV over 10 years).

Ongoing costs to public sector organisations of complying

62. There will be some ongoing training costs and staff time costs for public sector organisations to interact with the government based on new regulations and other new staff training.

Total Cost for Option 1

63. The estimated total costs of Option 1 lie between **£1.5** to **£8.5 million**, with a central estimate of **£5.3 million** (PV) over 10 years.

Table 11, Cost of Option 1, £ million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	1.0
	Public Sector Familiarisation Costs	0.0
	Public sector setup costs	Not monetised
Ongoing	Administration Costs	None
	Additional recovery costs	Not monetised
	Compliance Costs	Not monetised
	Public sector running costs	4.3
Total		5.3

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

64. Option 1 is not expected to have any set-up benefits.

Ongoing benefits

65. The objective of Option 1 is to reduce the amount of money flowing to ransomware criminals and deter criminals from attacking UK organisations.

66. In the most likely scenario, it is expected that the number of ransomware payments made will be dramatically lower, meaning that the flow of money to ransomware

criminals will also be much lower. Once the ransomware criminals learn this, and assuming that they expect this to continue in the long term, this significantly reduces incentive to attack for financially motivated attackers over the long term.

67. There are also benefits to organisations from a lower level of ransomware attacks. For example, lower ransomware insurance costs, lower data loss costs or lower recovery costs, and a lower chance of being the victim of a ransomware attack.

Option 2: A targeted ban on ransomware payments for regulated CNI and the public sector.

68. A ban on payments for certain sectors, namely the public sector and CNI. This would be an extension of the government's current position, where no government (HMT) funds can be used to pay a ransom. This proposal is a variation of Option 1, which encompasses all sectors.

69. It is expected that main drivers of costs will be the similar to Option 1. The difference will be in the magnitude since Option 1 covers the entire business population, whilst Option 2 covers only CNI and the public sector. If Option 2 were to be set up, ongoing costs to the government would be expected to be lower due to lower complexity, and net costs to business are expected to be lower due to fewer businesses in scope.

COSTS

Set-up Costs

Private Sector Costs

Familiarisation costs to the CNI sector

70. It is anticipated that relevant staff in reading organisations would have to familiarise themselves with the changes and read relevant information provided by the government. These costs are set out in table 3 above.

Public Sector Costs

Public Sector Monitoring and Enforcement Costs

71. The government anticipates that there will be some basic costs required to setup an effective monitoring and enforcement regime in order to oversee the organisations within the scope of the partial ban. This will likely centre around staffing and perhaps an IT system. Those working in monitoring and enforcement will need to be trained.

72. Public servants working in this area will need to read and understand how the partial ban will work. There will be a small-time cost for reading and processing any implications. This cost is expected to be negligible.

Familiarisation costs to public sector organisations to comply with the regime

73. The government anticipates that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information

provided by the government such as the guidance. These costs are set out in table 4 above.

Ongoing Costs

Private Sector Costs

Ongoing costs to private regulated CNI organisations of complying

74. There will be some ongoing training costs and staff time costs for private regulated CNI organisations to interact with the government based on new regulations and other new staff training.

Increase in attacks on sectors unaffected by the ban

75. It is possible that if successfully discouraged and deterred from targeting CNI, criminals may increase attacks on other UK sectors.

Additional recovery costs to CNI or public sector

76. It is likely that until attackers learn that the in scope specific sectors won't pay, they will continue attacks. If payments are banned, then recovery from ransomware attack for chosen businesses and public bodies will be more costly than the ‘Do nothing’ option. The additional costs from this policy would predominately be for any CNI organisations included in the scope since local authorities are already not allowed to use central government funds to pay ransoms.

Public Sector Costs

Cost of maintaining the capability to monitor and enforce the ban

77. Once the monitoring and enforcement regime is set up there will be operational costs, in the main staffing to monitor and advise organisations, and the maintenance of any IT. A proxy for this cost is set out above in the appraisal section under the heading ‘Public Sector Running costs’.

78. Total public sector running costs lie in a range of **£1.0** to **£3.2 million**, with a central estimate of **£2.1 million** (PV over 10 years).

Ongoing costs to public sector organisations of complying

79. There will be some ongoing training costs and staff time costs for public sector organisations to interact with the government based on new regulations and other new staff training.

Total Cost for Option 2

80. The estimated total costs of Option 2 lie between £0.97 to £3.3 million, with a central estimate of £2.1 million (PV) over 10 years.

Table 12, Cost of Option 2, £ million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	0.01
	Public Sector Familiarisation Costs	0.00
	Public sector setup costs	Not monetised
Ongoing	Administration Costs	None
	Additional recovery costs	Not monetised
	Compliance Costs	Not monetised
	Public sector running costs	2.1
Total		2.1

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

81. Option 2 is not expected to have any set-up benefits.

Ongoing benefits

82. The objective of Option 2 is to reduce the amount of money flowing to ransomware criminals and deter criminals from attacking UK organisations.

83. In the most likely scenario, the government expects that the number of ransomware payments made will be dramatically lower, meaning that the flow of money to ransomware criminals will also be much lower. Once the ransomware criminals learn this, and assuming that they expect this to continue in the long term, this significantly reduces incentive to attack for financially motivated attackers over the long term.

84. If successfully discouraged and deterred from targeting CNI, criminals may increase attacks on other UK sectors. This would still mean less critical CNI or national security impacts. Decreasing the likelihood of attacks in certain sectors is still worthwhile, as no measure can stop ransomware entirely. The ransomware attacks could also instead be displaced outside of the UK entirely, reducing harms to the UK.

85. There are also benefits to CNI and the public sector from a lower level of ransomware attacks. This may include lower ransomware insurance costs, lower data loss costs or lower recovery costs for example.

Option 3: A ransomware payments prevention regime for all other ransomware payments.

86. Whilst payments would remain legal, the government could criminalise payments not reported into and reviewed by the government ahead of time. This would increase government's understanding of payments and could prevent a payment should that be appropriate.

COSTS

Set-up Costs

Private Sector Costs

Familiarisation costs to private organisations of ensuring compliance

87. The government anticipates that relevant staff in reading organisations would have to familiarise themselves with the changes and read relevant guidance provided by the government. These costs are set out in Table 2.

Public Sector Costs

Cost of creating the capability to monitor and enforce the regime

88. There will be costs to setup a review regime which responds sufficiently quickly and can guide businesses through the process. This will likely centre around staffing, an IT system and engaging with affected organisations.

89. Public servants working in this area will need to read and understand how the regime will work. There will be a small-time cost for reading and processing any implications. This cost is expected to be negligible, but through the consultation a final option will be decided and any documentation to be read by public servants will be written. This cost may be updated in the following consultation responses to include a small awareness time cost.

Familiarisation costs to public sector organisations to comply with the regime

90. The government anticipates that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information and guidance. These costs are set out in table 4 above.

Ongoing Costs

Business Costs

Businesses administration costs when reporting.

91. When businesses need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the rationale and formula outlined in the main appraisal section above under the heading ‘Administration costs related to information submissions’.

Table 13, Option 3 Private Sector Administration costs for information submissions over 10 years, 2024.

Estimate	Number of information submissions (yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£million)
Low	283	0.5	15.87	**0.02**
Central	656	0.75	15.87	**0.07**
High	1,430	1	15.87	**0.21**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

92. Total private sector administration costs lie in a range of **£0.02** to **£0.21 million**, with a central estimate of **£0.07 million** (PV over 10 years).

Public Sector Costs

Running costs of the capability to monitor and enforce the regime

93. There will be running costs for the review regime. This will include staff costs, IT costs and engaging with affected organisations. A proxy for this cost is set out above in the appraisal section under the heading 'Public Sector Running costs'.

94. Total public sector running costs lie in a range of **£5.2** to **£21.6 million**, with a central estimate of **£17.3 million** (PV over 10 years).

Costs to public sector organisations to comply with the regime

95. The government assumes Options 3 and 4 will incur zero public sector submission costs because we assume that public sector organisations cannot pay a ransom. This is due to the government's current position, where no HMT funds can be used to pay a ransom.

Total Cost for Option 3

96. The estimated total costs of Option 3 lie between **£5.4** to **£24.9 million**, with a central estimate of **£18.3 million** (PV) over 10 years.

Table 14, Cost of Option 3, £ million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	1.0
	Public Sector Familiarisation Costs	0.0
	Public sector setup costs	Not monetised
Ongoing	Private Administration Costs	0.1
	Public Sector Administration Costs	None
	Additional recovery costs	None
	Compliance Costs	Not monetised
	Public sector running costs	17.3
Total		**18.3**

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

97. Option 3 is not expected to have any set-up benefits.

Ongoing benefits

98. The government expects that the increased knowledge of payments and interactions with attackers as a direct result of the review regime will improve the government's intervention. This compares to a baseline of very limited knowledge due to low reporting rates.

99. Due to increased volume of payments seen by the government, an increased rate of stopping payments to groups which will use funds for other harm to UK (terrorism, etc.) is expected because such ransom payments observed through the review regime will not be allowed.

Option 4: Mandatory reporting of a payment prior to the transaction

100. This option would require the reporting of a ransom payment prior to it being made. However, there would be no review or approval process, in contrast to Option 3. (for example, payments will not be blocked due to this process)

COSTS

Set-up Costs

Private Sector Costs

Familiarisation costs to private organisations of ensuring compliance

101. The government anticipates that relevant staff in reading private organisations would have to familiarise themselves with the changes and read relevant guidance provided by the government. These costs are set out in Table 2.

Public Sector Costs

Cost of creating the capability to monitor and enforce reporting

102. There will be costs to setup a mechanism which can guide businesses through the process. This will likely centre around staffing, perhaps an IT system and engaging with affected organisations.

103. Public servants working in this area will need to read and understand how the reporting will work. There will be a small-time cost for reading and processing any implications. The government expects this cost to be negligible, but through the consultation a final option will be decided and any documentation to be read by public servants will be written. This cost may be updated in the following consultation responses to include a small awareness time cost.

Familiarisation costs to public sector organisations to comply with the regime

104. The government anticipates that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information provided by the government. These costs are set out in table 4.

Ongoing Costs

Private Sector Costs

Private Sector administration costs when reporting

105. As and when businesses need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the general rationale and formula outlined in the main appraisal section above under the heading 'Administration costs related to information submissions'.

Table 15, Option 4 Private Sector Administration costs for information submissions over 10 years, 2024.

Estimate	Number of information submissions	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£ million)
Low	283	0.5	15.87	**0.02**
Central	656	0.75	15.87	**0.07**
High	1,430	1	15.87	**0.21**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

106. Total private sector administration costs lie in a range of **£0.02** to **£0.21 million**, with a central estimate of **£0.07 million** (PV over 10 years).

Ongoing compliance

107. There will be a small ongoing cost of remaining up to date with the reporting regulation. This will include staff training costs.

Public Sector Costs

Running cost of the capability to monitor and enforce the regime

108. There will be running costs for the reporting mechanism. This will include staff costs, IT costs and engaging with affected organisations. A proxy for this cost is set out above in the appraisal section under the heading 'Public Sector Running costs'.

109. Total public sector running costs lie in a range of **£3.9** to **£13.0 million**, with a central estimate of **£8.4 million** (PV over 10 years).

Costs to public sector organisations to comply with the regime

110. The government assumes Options 3 and 4 will incur zero submission costs because we assume that public sector organisations cannot pay a ransom. This is due to the government's current position, where no HMT funds can be used to pay a ransom.

Total Cost for Option 4

111. The estimated total costs of Option 4 lie between **£4.1** to **£16.3 million**, with a central estimate of **£9.5 million** (PV) over 10 years.

Table 16, Cost of Option 4, £million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	1.0
	Public Sector Familiarisation Costs	0.0
	Public sector setup costs	Not monetised
Ongoing	Private Administration Costs	0.1
	Public Sector Administration Costs	None
	Additional recovery costs	None
	Compliance Costs	Not monetised
	Public sector running costs	8.4
Total		**9.5**

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

112. Option 4 is not expected to have any set-up benefits.

Ongoing benefits

113. Any level of mandatory reporting will increase the government's awareness and understanding of the threat landscape. The government expects that the mandatory reporting of payments would be complementary to the other options set out in this OA or to other enforcement measures, since in isolation it will not substantively change the status quo. That is to say that there are not substantial direct benefits from this option.

Option 5: A mandatory reporting regime for all sectors.

114. Victims of a ransomware attack should report the incident to the reporting mechanism within a mandatory timeframe.

COSTS

Set-up Costs

Private Sector Costs

Standing up sufficient resources

115. Private organisations will need to plan how they will allocate sufficient resources to enable the submission of a compliant report within the required timeframe.

Private Sector Familiarisation Costs

116. The government anticipates that relevant staff in reading organisations would have to familiarise themselves with the changes and read the guidance provided by the government. For smaller organisations, it is expected that there will be a lower rate of familiarisation through permanent employees, and that instead this cost would be fed through the cost of employing cybersecurity experts who would be familiar with the guidance.

Public Sector Costs

Improvements to the reporting mechanism

117. The government will need to allocate initial additional resources to the reporting mechanism so that the reporting mechanism can advise, accept, and monitor reports. Any additional support that the government provides on receipt of a report will need to be setup.

Familiarisation costs to public sector organisations to comply with the regime

118. The government anticipates that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information provided by the government. These costs are set out in table 4.

Ongoing Costs

Private Sector Costs

Private Sector administration costs when reporting.

119. As and when businesses need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the rationale and formula outlined in the main appraisal section above under the heading 'Administration costs related to information submissions'.

Table 17, Option 5 Private Sector Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (per year)	Average time to submit (hours)	Hourly cost (£)	Estimated cost to business (£ million)
Low	858	0.5	15.87	**0.06**
Central	2,984	0.75	15.87	**0.33**
High	13,002	1	15.87	**1.9**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

120. Total private sector administration costs lie in a range of **£0.06** to **£1.9 million**, with a central estimate of **£0.33 million** (PV over 10 years).

Public Sector Costs

Running cost of the capability to monitor and enforce the regime

121. The government will need to allocate permanent additional resources to the reporting mechanism so that the reporting mechanism can advise, accept, and monitor reports. This will include staff and IT costs. A proxy for this cost is set out above in the appraisal section under the heading 'Public Sector Running costs'.

122. Total public sector running costs lie in a range of **£1.3** to **£5.4 million**, with a central estimate of **£4.3 million** (PV over 10 years).

Public Sector administration costs when reporting.

123. As and when public sector organisations need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the rationale and formula outlined in the main appraisal section above under the heading 'Administration costs related to information submissions'.

Table 18, Option 5 Public Sector Administration costs related to information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (Yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£'000)
Low	40	0.5	15.87	**3.0**
Central	86	0.75	15.87	**9.4**
High	187	1	15.87	**27.4**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

124. Total private sector administration costs lie in a range of **£3,000** to **£27,400**, with a central estimate of **£9,400** (PV over 10 years).

Total Cost for Option 5

125. The estimated total costs of Option 5 lie between **£1.6** to **£10.4 million**, with a central estimate of **£5.6 million** (PV) over 10 years.

Table 19, Cost of Option 5, £million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	1.0
	Public Sector Familiarisation Costs	0.0
	Public sector setup costs	Not monetised
Ongoing	Private Administration Costs	0.3
	Public Sector Administration Costs	0.0
	Additional recovery costs	None
	Compliance Costs	Not monetised
	Public sector running costs	4.3
Total		**5.6**

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

126. Option 5 is not expected to have any set-up benefits.

Ongoing benefits

127. The main benefit is that the data received from the reports will improve the government's knowledge and understanding of the threat landscape. This will be achieved through an increased reporting rate because compared to the 'Do nothing' option reporting will change to mandatory, and the base level of reporting is low.

Option 6: Mandatory reporting of ransomware incidents for specific sectors

128. Victims of a ransomware attack in specific sectors (assumed in this appraisal to be CNI all public sector organisation) should report the incident to the reporting mechanism within a mandatory timeframe.

129. The government expects that the main drivers of the costs and benefits of Option 6 will be similar to Option 5, except that there will likely be lower costs as less organisations are in scope, and lower informational benefits due to the incomplete picture from receiving reports limited to in-scope sectors only.

130. Setup and ongoing costs to the government are expected to be lower due to less complexity, and net costs to business are expected to be lower due to fewer businesses in scope. For benefits, the government's knowledge of the threat landscape will be lower as compared to Option 5.

COSTS

Set-up Costs

Business Costs

Standing up sufficient resources

131. Private organisations in the affected sectors will need to plan how they will allocate sufficient resources to enable the submission of a compliant report within the required timeframe.

Private Sector Familiarisation Costs

132. The government anticipates that relevant staff in reading organisations would have to familiarise themselves with the changes and read relevant information provided by the government. For smaller organisations, it is expected that there will be a lower rate of familiarisation through permanent employees, and that instead this cost would be fed through the cost of employing cybersecurity experts who would be familiar with the guidance.

Public Sector Costs

Improvements to the reporting mechanism.

133. The government will need to allocate initial additional resources to the reporting mechanism so that the reporting mechanism can advise, accept, and monitor reports. Any additional support that the government provides on receipt of a report will need to be setup.

Familiarisation costs to public sector organisations to comply with the regime

134. It is anticipated that relevant staff in reading public sector organisations would have to familiarise themselves with the changes and read relevant information provided by the government. These costs are set out in table 4 above.

Ongoing Costs

Business Costs

Businesses administration costs when reporting.

135. As and when businesses need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the rationale and formula outlined in the main appraisal section above under the heading 'Administration costs related to information submissions'.

Table 20, Option 6 Private Sector Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (per year)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£'000)
Low	9	0.5	15.87	**0.63**
Central	30	0.75	15.87	**3.3**
High	130	1	15.87	**19.1**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

136. Total administration costs lie in a range of **£630** to **£19,100**, with a central estimate of **£3,300** (PV over 10 years).

Public Sector Costs

Running cost of the capability to monitor and enforce the regime

137. The government will need to allocate permanent additional resources to the reporting mechanism so that the reporting mechanism can advise, accept and monitor reports. This will include staff and IT costs. A proxy for this cost is set out above in the appraisal section under the heading 'Public Sector Running costs'.

138. Total public sector running costs lie in a range of **£1.0** to **£3.2 million**, with a central estimate of **£2.1 million** (PV over 10 years).

Public Sector administration costs when reporting.

139. As and when public sector organisations need to report a ransomware attack, they will incur costs in terms of staff hours needed to compile the required information and to liaise with the reporting mechanism. The costs are estimated below, with the rationale and formula outlined in the main appraisal section above.

Table 21, Option 6 Public Sector Administration costs for information submissions over 10 years, FY 2024/25.

Estimate	Number of information submissions (Yearly)	Average time to submit (hours)	Hourly cost (£, 2022/23 prices)	Estimated cost to business (£'000)
Low	40	0.5	15.87	**3.0**
Central	86	0.75	15.87	**9.4**
High	187	1	15.87	**27.4**

Source: ASHE 2020 Table 14.5a, Data security incident trends | ICO, Home Office Internal Analysis.

140. Total administration costs lie in a range of **£3,000** to **£27,400**, with a central estimate of **£9,400** (PV over 10 years).

Total Cost for Option 6

141. The estimated total costs of Option 6 lie between **£1.0** to **£3.3 million**, with a central estimate of **£2.1 million** (PV) over 10 years.

Table 22, Cost of Option 6, £ million PV over 10 years

		£ million
Setup	Private Familiarisation Costs	0.0
	Public Sector Familiarisation Costs	0.0
	Public sector setup costs	Not monetised
Ongoing	Private Administration Costs	0.0
	Public Sector Administration Costs	0.0
	Additional recovery costs	None
	Compliance Costs	Not monetised
	Public sector running costs	2.1
Total		**2.1**

Source: Home Office Internal Analysis

BENEFITS

Set-up benefits

142. Option 6 is not expected to have any set-up benefits.

Ongoing benefits

143. The main benefit is that the data received from the reports will improve the government's knowledge and understanding of the threat landscape. This will be achieved through an increased reporting rate because compared to the 'Do nothing' option reporting will change to mandatory, and the base level of reporting is low.

Overall Costs and Benefits

144. Table 23 outlines the indicative measures that might be used to measure the level of benefits achieved by the chosen options. The measures are set out against the strategic objectives to provide a clear summary of where the benefits lie. The breakdown of strategic objectives into each option is set out in section 6: Description of shortlisted policy options carried forward.

Table 23, Summary of indicative measures of benefits by strategic objective.

Strategic Objective	Secondary objective / Benefit	Indicative Measure
1. Reducing the amount of money flowing to ransomware criminals and deterring criminals from attacking UK organisations.	Reduction in the percentage of UK organisations paying ransoms.	• Measurable reduction in the value and number of ransom payments made by UK businesses baselined for the first year of reporting compared to subsequent years.
2. To increase operational partners ability to disrupt and investigate ransomware actors by increasing the Home Office's visibility and knowledge of the ransomware payment landscape.	A reduction in repeat attacks on victims either by the same criminal or ransomware strand.	• The number of disruptions and investigations made by law enforcement against ransomware actors baselined for the first year of the intervention compared to subsequent years. • Survey of improvement of law enforcement understanding of the ransomware payment landscape post intervention compared to pre intervention.
3. To increase the government's knowledge and understanding of the threat landscape.	Improve the ransomware evidence base.	• Improve the evidence base scores for ransomware.

Table 24, Summary of Costs by option, £ million

Costs (£ million), by option	0 ('Do nothing')	1	2	3	4	5	6
Total set up costs	-	1.0	0.02	1.0	1.0	1.0	0.02
Total ongoing costs	-	4.3	2.1	17.4	8.5	4.7	2.1
Total costs	**-**	**5.3**	**2.1**	**18.3**	**9.5**	**5.6**	**2.1**

Source: Home Office Internal Analysis

Sensitivity Analysis

145. In table 25 a range of decreases in the likelihood of previously costed worst-case ransomware scenarios occurring are explored in sensitivity analysis, these include the NHS WannaCry attack (2017) and the previously noted Cambridge Centre for Risk Studies SE electricity attack[65].

146. The monetary values represent the savings, in terms of reduced harm, to the UK from a given per cent decrease in likelihood of a given scenario. These are for illustrative purposes to show the range of potential benefits that might be realised if an option as listed in this OA were to have such an effect.

147. Higher decreases in likelihood (for example, 50 per cent compared to 25 per cent) lead to higher avoided costs, so there is more chance of breakeven in table 26 below.

Table 25, Reduced cost to UK for a range of decreases in likelihood of a worst-case scenario (£ million, non-discounted).

Per cent % change in likelihood of worst-case scenario	1%	5%	10%	25%	50%
WannaCry[66]	0.09	0.5	0.9	2.3	4.6
SE Electricity Grid (S1 scenario)	9.6	48.0	96.0	240.0	480.0

Source: Home Office Internal Analysis

[65] Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy; Cambridge Risk Framework series; Centre for Risk Studies, University of Cambridge, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf

[66] Page 14, Securing cyber resilience in health and care: October 2018 update - GOV.UK (www.gov.uk) https://assets.publishing.service.gov.uk/media/5bbe1250ed915d732b99254c/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf

Table 26, breakeven test of the benefits of a range of decreases in the likelihood of a SE electricity grid cyber-attack ('S1' scenario) compared to the high scenario estimated cost of this legislation.[67]

Test: is benefit from loss reduction greater than total cost of chosen proposals?			
	(direct losses)	Central (indirect losses)	High (total GDP @Risk)
1%	No	No	No
5%	Yes	Yes	Yes
10%	Yes	Yes	Yes
25%	Yes	Yes	Yes
50%	Yes	Yes	Yes

Source: Home Office Internal Analysis

148. Table 26 draws on the study by the Cambridge Centre for Risk Studies introduced in section 2. It uses figures from the least disruptive 'S1' scenario that was modelled to show the economic effects of a well-resourced attack on the electricity grid in the south and east of the UK.

149. A breakeven test is conducted of the benefits of a range of decreases in the likelihood of the 'S1' scenario compared to the high scenario for the estimated total cost of this OA's proposals (Options 1, 3 and 5, which is £29.3 million). The expected frequency of the attack is set at one per cent per year. The calculation of the benefit is:

expected yearly losses x frequency of attack x decrease in likelihood of scenario x number of years (10).

150. Although table 26 is largely illustrative, it does demonstrate the potential for large direct and indirect costs savings, as well as reduced wider economy effects from the proposed legislation.

151. This style of analysis is particularly useful since the interventions aim to reduce the risk of attacks with large scale, economy wide harms.

Value for money (VfM)

152. Whilst no benefits have been quantified at the point of consultation, it can be seen in the sensitivity analysis section and supported by the background section that the most disruptive ransomware attacks are incredibly expensive to business, CNI and the public sector.

153. A reduction in the instances of ransomware attacks, or the severity of attacks through the policy options outlined in this assessment will have the potential to cover costs.

[67] As introduced in section 2 of this OA. Integrated Infrastructure: Cyber Resiliency in Society, Mapping the Consequences of an Interconnected Digital Economy (Centre for Risk Studies, University of Cambridge). https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-integrated-infrastructure-cyber-resiliency-in-society.pdf

Impact on small and micro-businesses

154. Option 1, a complete ban on ransomware payments, may disproportionally impact small and micro businesses for which the only option following a ransomware attack is to pay to decrypt data, and which cannot afford specialist ransomware insurance, or clean up specialists.

155. For Option 2, a targeted ban on ransomware payments for regulated CNI and the public sector. It is assumed that due to the nature of the CNI and public sectors that this option will not have a disproportionate impact on SMBs. The removal from scope of the CNI supply chain further mitigates possible impacts as more SMBs would be captured in such a business population. The Home Office will take consultation responses into account to ensure all effects are captured and all possible mitigations are considered.

156. For Option 3, a payment prevention regime for all other ransomware payments. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. The Home office aims to mitigate possible impacts on by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects are captured and all possible mitigations are considered.

157. For Option 4, the mandatory reporting of a payment prior to the transaction. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. However, as Option 4 will require less business capacity to complete than Option 3, impacts are assumed to be smaller. The Home Office aims to mitigate possible impacts on SMBs by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects are captured mitigations are considered.

158. For Option 5, a mandatory reporting regime for all sectors. It is possible that this option may have disproportionate impact on SMBs. SMBs will have less employee capacity during an attack to engage with the government. The Home office aims to mitigate possible impacts on by designing a simplified and time efficient process. The Home Office will take consultation responses into account to ensure all effects are captured and all possible mitigations are considered.

159. For Option 6, the mandatory reporting of ransomware incidents for specific sectors. It is assumed that due to the nature of the CNI that this option will not have a disproportionate impact on SMBs. The Home Office will take consultation responses into account to ensure all effects are captured and all possible mitigations are considered.

160. As shown in section: background, small businesses are more likely than other sectors of the business population to have policies against paying ransoms. Small and Micro businesses are also more likely to benefit from any reduction in the risk of being ransomware attacked for the same reasons.

Statutory Equalities Duty

All Consultation OAs are required to have the Statutory Equalities Duty reviewed by the SRO before signoff.

Mandatory specific impact test - Statutory Equalities Duties	Complete
Statutory Equalities Duties The overriding strategic objective of the proposed interventions are to reduce cyber crime and the associated harms to UK businesses, reducing the threat of ransomware attacks by making the UK a less attractive target to ransomware criminals. Simultaneously, the Home Office is looking to shore up the most crucial parts of the UK economy, reducing the national security threat that ransomware poses. The Home Office are aware that criminals often exploit vulnerable people and businesses. However, there is no evidence that the risk of exploitation for this offence is or will be higher than in other crimes. There is limited evidence available when considering due regard for public-sector equality in relation to the provision. The Home Office are confident that this will not have a discriminatory effect against any of the considered protected characteristics. Overall, the Home Office believe the benefits of these policies outweigh the potential risks. By placing more emphasis on reducing the impacts of ransomware, the burden of crime prevention is reduced for the public. This allows all, including those in protected characteristic groups, to engage in everyday internet use more safely and without exclusion. Individuals and business owners who could have been a victim of a crime due will be positively impacted through reduced criminality. The Home Office will take consultation responses into account to ensure all effects are captured and all possible and proportionate mitigations are enacted. **The SRO has agreed these summary findings.** *(you must get SRO agreement here)*	**Y**