Written evidence submitted by His Majesty's Government

Introduction

1. His Majesty's Government (HMG) is submitting a response to the Joint Committee on the National Security Strategy's Call for Evidence to support the Inquiry into Ransomware.

2. Ransomware is a top priority for Government and is a novel and complex threat type that has continued to intensify and evolve, with the number of attacks, both in the UK and globally, assessed by the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC) to be increasing[1]. It involves highly technically sophisticated and dynamic cyber criminals who operate one of two broad modus operandi in targeting victims. They either commit widespread opportunistic attacks against often poorly protected parts of the UK economy, or specifically target critical national infrastructure to cause maximum harm.

3. Ransomware actors prevent access to systems and steal sensitive data, threatening to leak it publicly (often via the dark web) in a two-stage extortion approach. Many actors also operate a ransomware-as-a-service (RaaS) model whereby criminals can rent or lease strains to deploy, thus reducing the level of expertise required to conduct an attack, whilst also complicating attribution.

4. Ransomware actors often operate from safe havens outside our jurisdiction, including in Russia where they operate with impunity. The threat they pose is exacerbated because ransomware payments are largely made in lightly regulated cryptocurrencies which are difficult to trace.

5. HMG acknowledges that ransomware is a serious threat, and therefore has been working for a number of years to build a mature response to cyber threats, and ransomware specifically. We have undertaken comprehensive work in this space, including what was set out in the National Cyber Strategy (2016-2021), HMG launched a cross-Government ransomware "sprint" that ran from June 2021 to February 2022. The sprint[2] involved a number of Whitehall Departments[3], operational partners[4] and law enforcement[5]. It explored existing ransomware policies, areas of potential improvement, and culminated with a series of recommendations to Ministers. Since then, the Home Office has continued to lead cross-Government ransomware work under the Threat Pillar of the National Cyber Strategy.

---

[1] Decoding 2021, NCSC-A, NCA
[2] The Ransomware Sprint was a focused campaign to accelerate our response to this growing threat in June 2021.
[3] Home Office, Cabinet Office, Department for Digital, Culture, Media and Sport, HM Treasury, Foreign, Commonwealth and Development Office, Attorney General's Office and the Department for Business, Energy and Industrial Strategy.
[4] The National Cyber Security Centre
[5] The National Crime Agency and City of London Police

6. This work has been particularly timely given the change in the threat picture as a result of Russia's war with Ukraine. We know that the Russian State is one of the world's most prolific cyber actors and dedicates significant resource towards conducting cyber operations around the globe. They have undertaken a range of attacks[6] in support of their illegal invasion in February, and the National Cyber Security Centre (NCSC) has confirmed that Russian cyber activity has included attempted cyber attacks against the UK media, telecommunications and energy infrastructure.

7. Our evidence, set out below, focuses on the topics for which the Committee has invited evidence, and has been compiled by the Home Office (HO) with the support of the Cabinet Office (CO), the Centre for the Protection of National Infrastructure (CPNI), the Department for Business, Energy and Industrial Strategy (BEIS), the Department for Digital, Culture, Media & Sport (DCMS), the Foreign, Commonwealth & Development Office (FCDO), HM Treasury (HMT), the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC). We outline the work completed both under the sprint and more recently, as well as the opportunities and challenges that were faced. However, because of the security classification of this evidence, the response does not provide full details about specific policy work and live operations.

HMG's approach to cyber threats

8. The government's approach to tackling cyber threats, including the threat from ransomware, is set out in the National Cyber Strategy (2022). The strategy builds on the commitments made in the Integrated Review of Security, Defence, Development and Foreign Policy to cement the UK's position as a responsible and democratic cyber power and sets out the government's approach to protecting and promoting the UK's interests in cyberspace.

9. The National Cyber Strategy highlighted ransomware as the most significant cyber threat facing the UK, and it still is. The strategy commits £2.6bn of new investment to deliver objectives under five strategic pillars:
   a) **Eco-System** - Strengthening the UK cyber ecosystem by investing in cyber skills, deepening partnerships between government, academia and industry, and strengthening UK cyber exports.
   b) **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.
   c) **Technology** - Taking the lead in the technologies vital to cyber power by building our industrial capability and sustaining advantage in security technologies critical

[6] Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion - GOV.UK (www.gov.uk)

to cyberspace (including microprocessor design, operational technologies and cryptography).

d) **International** - Advancing UK global leadership and influence towards a more secure, prosperous and open international order, sharing the expertise that underpins UK cyber power.

e) **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.

10. This broad and multifaceted response necessarily requires support from multiple ministers and departments but is led by The Chancellor of the Duchy of Lancaster (CDL) and the Home Secretary. CDL provides overall leadership across departments to ensure an effective government response to cyber threats, including the implementation of the National Cyber Strategy, and has overall responsibility for the cyber security and resilience of the UK's Critical National Infrastructure. The Home Secretary has specific responsibility to counter cyber crime and, as part of this, leads the government response to the ransomware threat.

The extent and nature of the ransomware threat (including sources), modes of extortion, and how the threat could evolve in future.

11. The National Crime Agency (NCA) and the National Cyber Security Centre (NCSC) define ransomware as a malicious software that can encrypt the victim's files, holding the data hostage until a ransom is paid, often in Bitcoin or other cryptocurrency. Ransomware attacks can be existential threats to victims, leading to business closure, inaccessible public services and compromised data. This aligns closely with international definitions[7]. Ransomware actors do not constrain their attacks to any particular sector or business – it includes small and large businesses, Critical National Infrastructure (CNI), local government organisations, hospitals, schools and other sectors.

12. The NCA's National Cyber Crime Unit (NCCU) states that ransomware has evolved from a niche cyber crime problem to a national security issue in a short period of time. The number of ransomware groups impacting the UK has expanded considerably, and it is now the most significant cyber threat to the UK. This is reiterated in the NCSC's Annual Review 2022, which reports that over the last year the cyber security threat to the UK has evolved significantly and assesses ransomware to be one of the most significant cyber security threats facing businesses and organisations in the UK[8].

[7] For example, the US's recent legislated definition of 'ransomware attack' as per the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Cyber Incident Reporting for Critical Infrastructure Act of 2022 (cisa.gov)

[8] NCSC Annual Review 2022

13. We are aligning this work with our State Threats Strategy, as it is important for us to use as many levers as we can to target ransomware and cyber crimes more broadly. Particularly, as we know that Russian-language Organised Crime Groups (OCGs) and actors, largely but not always based in former-Soviet states, continue to pose the most significant cyber crime threat. It is almost certain that the deployment of the highest impact malware (including ransomware) affecting the UK remains concentrated mostly in Russia. This, along with the recent war in Ukraine, increases the complexity of combatting the ransomware threat.

14. It is difficult to understand the nature of the connections between the Russian state and any OCG at any point in time, as the Russian state rarely intervenes or cooperates with international law enforcement. However, it is reasonable to conclude that the criminal profits made by Russian ransomware OCGs would bring them to the attention of the state. As such, state involvement would vary from knowledge of ransomware OCGs' criminal activity and allowing them to operate with impunity, to more direct links, such as the deep relationship between ransomware group Evil Corp and the Russian Federal Security Service (FSB).

15. We know that ransomware actors are financially motivated, and that ransomware payments and the cryptocurrency system which underlies them have enabled the ransomware threat to advance. We are working across Government to reduce the flow of money to ransomware actors (see paragraph 56 for further detail).

16. Ransomware attacks cause layers of harm. In the first instance they disrupt crucial services whilst the attack is taking place. Subsequent harm is caused by actors exfiltrating data and threatening to misuse it or publish it online if a ransom is not paid. This, combined with encryption of a victim's systems, is often referred to as 'double extortion'.

17. There can therefore be a significant social cost from ransomware attacks, especially if public services and infrastructure are impacted. Consequently, many victims choose to pay the ransom rather than risking disruption to their customers or organisation, and a large quantity of attacks go unreported, obscuring the true picture of the threat.

18. Most ransomware actors are highly technically sophisticated and have extremely high levels of cyber skills. Ransomware actors develop their own versions of ransomware, known as 'variants' or 'strains', and can undergo rebranding to indicate a change to software or threat actor. Some ransomware actors have diversified their revenue streams using a Ransomware-as-a-Service (RaaS) business model and sell access to their ransomware schemes on the dark web or outsource ransomware distribution to affiliates in exchange for a percentage of the ransom. These affiliates have significantly lower cyber skills, and thus RaaS has lowered the barrier to entry and increased the availability of ransomware strains, increasing the frequency of ransomware attacks in recent years. Most of the highest threat ransomware strains are

highly likely to be operating as a RaaS model. As such, RaaS can complicate attribution of incidents due to the affiliates and/or freelancers that may be involved in conducting an attack.

19. This evolution is reflected internationally, as highlighted through the Joint Cyber Security Advisory (CSA) report[9] authored by the Federal Bureau of Investigation (FBI), US Cybersecurity and Infrastructure Security Agency (CISC), US National Security Agency, Australian Cyber Security Centre, and the UK's NCSC. This publication summarised that in 2021, cybersecurity authorities in the United States, Australia, and the UK observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organisations globally. It also found that ransomware actors' tactics and techniques continued to evolve in 2021, which reinforces ransomware actors' growing technological sophistication and an increased ransomware threat to organisations globally.

20. The ransomware threat to the UK continues to evolve, however, the broader evidence base on ransomware remains limited, both in the UK and globally. This is because of a range of factors, including the general underreporting of cyber crime (and ransomware specifically), the sophistication of ransomware attacks and broader academic evidence base being limited. This presents a challenge when exploring policy options to combat this threat. Despite this, we assess that it can cause the most significant harms due to the loss of data and services incurred by victims.

21. Alongside its allies, HMG encourages victims to report incidents. However, reporting is not currently mandatory in the UK. The NCA currently estimate that only about 2-10% of cyber crime is reported to HMG, making it one of the most underreported crime types in the UK. Increasing reporting of cyber crime is a priority as it enables us to build a better understanding of the threat and fight it more effectively. Reporting also enhances the NCCU's ability to manage and mitigate ransomware attacks.

22. There are many sources of statistics offering insight into the prevalence of cyber crime and ransomware incidents, but all sources are imperfect and can sometimes present contradictory findings. We do know, however, that ransomware accounted for 1.2% (291 out of 24,503) of cyber crimes reported to Action Fraud in Q3 2022. Additionally, the Crime Survey for England and Wales[10] estimated 641,000 incidents of computer misuse against adults in England and Wales in the year ending June 2022, of which 102,000 were computer virus incidents. The most recent estimates of 'ransomware' suggest there was a demand for money to release files in 0.5% of computer virus incidents against individuals in the year to March 2022.[11]

---

[9] 2021 Trends show increased globalised threat of ransomware.pdf (ncsc.gov.uk)

[10] The evidence base on ransomware remains limited, due to factors including the general underreporting of cyber crime, and the sophistication of ransomware attacks. The Crime Survey for England and Wales provides a tentative proxy indicator for the prevalence of ransomware against individuals.

23. In addition to this, the Cyber Security Breaches Survey (CSBS)[12] 2022 reports that of the 39% of UK businesses identifying a cyber breach or attack in the last 12 months, around 4% identified a ransomware attack. It also reports that the prevalence of ransomware has fallen year on year since 2017, with 17% of businesses who had identified a cyber breach identifying a ransomware attack in 2017 compared with 4% in 2022. However, despite its reported low prevalence, organisations still cited ransomware as a major threat, with 56% of businesses reporting that they had a policy not to pay ransoms, as advised by the Government.

24. The payment of a ransom to criminals is likely to encourage further criminal activity and does not guarantee a successful outcome for the victim. Paying a ransom does not protect networks, nor will it prevent the possibility of future data leaks. The decision whether or not to pay the ransom is ultimately a matter for the individual or organisations concerned. The Government strongly encourages victims of ransom demands to contact the authorities for support.

25. Each year, the NCSC manages the response to hundreds of incidents and works closely with the NCA on significant ransomware incidents[13]. Between September 2021 and August 2022, 63 incidents responded to by NCSC were deemed nationally significant. Of those, 18 were ransomware incidents requiring a nationally coordinated response led by the NCSC[14].

26. Externally, multiple industry bodies report ransomware to be a significant threat, with several reporting recent increases in the scale[15] or ransoms[16][17]. However, the scope and methodological quality of industry reports differs widely. There are also reports of a change in tactic from widespread attacks to more serious targeted attacks[18].

---

[11]ONS Crime in England and Wales: year ending March 2022

[12] The Cyber Security Breaches Survey (CSBS) provides official statistics on the proportion of businesses who experienced a cyber breach or attack, including ransomware It is representative of all sizes of the UK business population that predominantly consists of micro and small businesses. However, to counter this the study boosts survey responses from medium and large businesses and high income charities and focuses on large organisations in the qualitative strand. Please note that organisations can only report on breaches and attacks that they have detected thus the survey may have a tendency to underestimate the real level of breaches or attacks.

[13]New Cyber Attack categorisation system to improve UK... - NCSC.GOV.UK

[14] NCSC Annual Review 2022

[15] E.g. Sophos – State of ransomware, 2022; Cybereason – Ransomware: The true cost of business, 2022; Group IB – Ransomware uncovered, 2021

[16] The cost of ransomware in 2021: A country-by-country analysis (emsisoft.com); Sophos – State of ransomware, 2022;

[17] Developing accurate estimates about the scale and harms from ransomware is very challenging and the methodology behind industry estimates is often unclear. Industry estimates should be viewed with considerable caution and these figures should not be viewed as validated or endorsed by the Home Office. While the exact reasons for different estimates is not clear, the evidence base on ransomware is only emerging and there is considerable difference in the specific aspects of ransomware

[18] Ransomware by the numbers: Reassessing the threat's global impact | Securelist;

27. Therefore, whilst there are some indications that the number of incidents is decreasing (potentially in light of the current geopolitical backdrop), the number of ransomware incidents being referred to the NCA's NCCU Triage, Incident Coordination and Tasking (TICAT) team, has shown a steady gentle increase over the last two years. Work is ongoing with public and private sector partners to better understand ransomware trends.

Levels and sources of vulnerability of UK organisations to ransomware, including operators of critical national infrastructure.

28. The key to combating ransomware is better cyber resilience. Cyber hygiene, refers to a set of practices performed regularly to maintain the health and security of networks and data, is the cause of the vast majority of cyber attacks. People and organisations are not getting the basics right – poor configuration of devices and networks, poor patching of software, default passwords, and weak passwords. We need to stop letting ransomware into our systems so easily.

29. When looking at government approaches to ransomware, we need to ensure that better cyber resilience – making it harder for ransomware actors to access systems – is at the heart of our activities. A prosperous digital society needs to be resilient to cyber threats and equipped with the knowledge and capabilities required to maximise opportunities and manage risks. However:

a) 39% of UK businesses suffered a cyber attack over the past 12 months[19].
b) The UK ranked third behind the US and Ukraine in terms of incoming malicious cyber-activity linked to nation states between July 2020 to June 2021[20].
c) Modelling shows the implications of a major cyber attack in the UK could result in a 1.6% of GDP shock and £29 billion added to government borrowing[21].
d) The UK is heavily reliant on the internet and computers – 92% of adults use the internet[22] and 92% of businesses have some form of digital exposure[23].

30. HMG has a range of levers to combat this threat, and the Department for Digital, Culture, Media and Sport is specifically focused on improving the cyber resilience of organisations and businesses in the UK. They are ensuring that organisations have guidance to get strong cyber resilience measures in place, backed up by a system of corporate incentives, market forces that drive investment in cyber resilience and, where appropriate, regulation, to force organisations to act. They are particularly focused on securing supply chains, especially digital supply chains, as only 13% of

[19] Cyber Security Breaches Survey 2022
[20] Office for Budget Responsibility, 2022
[21] Office for Budget Responsibility, 2022
[22] Office for National Statistics, 2021
[23] Cyber Security Breaches Survey 2022

businesses and charities reviewed the risks posed by their immediate supply chains in the last 12 months[24].

31. Alongside this, the Centre for the Protection of National Infrastructure (CPNI) notes that some form of social engineering[25] such as phishing is used as an entry route by ransomware attackers, exploiting information that organisations make openly available. Therefore, CPNI have published guidance on security-minded social media management to help mitigate this threat.

32. CPNI have also worked with academics from the University of Bath and University of Bristol to test behaviours around phishing emails after developing a research tool called Phishtray[26]. In 2022/2023, CPNI undertook steps to further develop the tool to be more customer friendly. This enabled CPNI partners to test their workforce's susceptibility to phishing and spear-phishing emails, using anonymous data to feed into new real-world research to test new interventions developed by academics to better understand ways of preventing phishing emails from being successful.

33. We have seen recent attacks against CNI globally, including UK CNI. We have seen recent attacks against critical services globally. In the UK this includes an attack on a software supplier to the NHS, Advanced, and we have seen attacks on Medibank in Australia and CommonSpirit Health in the USA. HMG is working closely with CNI operators to achieve resilience against common attack methods and to put in place more advanced protections where appropriate.

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

Regulatory requirements placed on victims

34. For Operators of Essential Services designated under the Network and Information System (NIS) Regulations[27], this means at least meeting the baseline standard set by the relevant Competent Authorities for each sector. Under the National Cyber

[24] Cyber Security Breaches Survey 2022

[25] Social engineering, in the context of information security, is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

[26] Phishtray is a software to support academia and industry in creating protections against social engineering.

[27] The Network and Information System Regulations came into force on 10 May 2018.

Strategy, the Government committed to review its ability to hold CNI operators to account to ensure they invest in the cyber security of critical systems and effectively manage their risk. We are strengthening the regulatory framework, to improve its coverage, powers, and agility to adapt, within the context of broader national security risk and rapidly changing threat and technology. This began with a consultation on reforms to the NIS regulations and implementation of the new security framework for UK telecommunications providers. DCMS has now published HMG's response to this consultation[28].

35. To strengthen preparedness, the NCSC is expanding their accredited scheme for Cyber Incident Response companies and introducing a new scheme for exercising, which is of particular importance to CNI sectors. This includes ransomware-specific exercising to drive up awareness of the threat and strengthen operators' ability to respond to an attack. It will also set out clear requirements for exercising and testing for adversary simulation across CNI operators.

36. HMG itself also undertakes regular internal cyber exercising. This is largely led at the departmental level and supported by the NCSC and NCCU. The NCSC exercising team coordinates an exercising cadre that comprises over 130 members from across government and the devolved administrations.

37. As previously outlined, it is not currently mandatory to report ransomware incidents in the UK, and ransomware payments are legal but strongly discouraged. This is provided that any payment does not breach any existing law concerning terrorist financing or a sanctioned actor. HMG and law enforcement strongly encourage incident reporting through Action Fraud, the national reporting facility for fraud and cybercrime and to the National Fraud Intelligence Bureau (NFIB). They are both operated by the City of London Police, the UK's National Lead Force for fraud and cyber crime. Victims of cyber attacks can also contact NCSC for immediate technical assistance.

38. Action Fraud is currently being reviewed by the Home Office and a procurement process, managed by City of London Police, is underway to improve the service and the victims' experience when reporting a cyber crime or fraud. The service will also provide victims with additional sources of support and guidance, integrating with the work of the NCSC and other organisations.

Victim experience

39. In the Cyber Security Breaches Survey 2022[29], interviewers spoke to organisations about the threat they believed ransomware posed to them, and the protections (or lack of) they had in place against it. There was variation amongst responding organisations

[28] Proposal for legislation to improve the UK's cyber resilience - GOV.UK (www.gov.uk)
[29] DCMS (2022) Cyber Security Breaches Survey (CSBS)

in how they viewed the threat of ransomware but participants tended to strongly believe that ransomware posed a high risk to their organisation. Ransomware was seen by some as a useful tool to highlight the risk of any kind of cyber attack. Many organisations cited reports of ransomware in the media making them more aware of the damage it could cause. Some believed that even though the level of damage could be high, the likelihood of getting attacked was low. Organisations that believed that ransomware posed no threat to them, did so because they thought their data was not valuable, or because they had their data backed up or stored in a cloud service.

40. Of those who had not been attacked by ransomware, organisations tended to have an incident response plan which involved shutting down infected systems and notifying staff and relevant parties. Some intended to notify authorities, although they often did not specify which authorities these were. Organisations were very concerned about the damage that a ransomware attack could do to their reputation, which some believed was worse than the cost of the attack itself. Of those who had been attacked, organisations mentioned a notable shift in how the organisation approached cyber security in the aftermath. There was particular emphasis on end-user behaviour.

41. There was a marked difference between large and small organisations in how they perceived the threat of ransomware. Smaller organisations tended to believe that ransomware did not pose a threat. This was because participants either believed it was unlikely to happen, or that they did not have anything of value. Organisations tended to have an informal plan in place in the event of an attack, which involved shutting down systems and re-booting with backed-up data. Smaller organisations often mentioned speaking to an IT provider for advice in the event of an attack. Some organisations had no plan at all. However, those small organisations which viewed ransomware as a serious threat had a strict plan in place in the event of an attack.

42. There was a clear difference in attitudes on whether or not an organisation would pay a ransom or not. Those that had not experienced an attack were extremely likely to say they would not pay under any circumstances. This was due to concerns around reputational damage and confidence that their back-up systems and incident management plans would cause minimal disruption. However, there were instances where those that had experienced a ransomware attack had paid a ransom, contrary to their policy. This was because, in reality, the disruption caused immediately impacted the organisation's continuity, so they paid the ransom to become fully operational as soon as possible. These organisations tended to be smaller with low confidence in their cyber security, so would pay the ransom as opposed to recovering systems themselves. They also had a lower risk of reputational damage.

Sources of prevention and detection

43. The NCSC operate a wide range of services alongside their comprehensive suite of advice and guidance including Early Warning, which is a free service offered to a wide range of organisations, designed to inform organisations of potential cyber-

attacks on their network. The service uses a variety of information feeds from the NCSC, trusted public, commercial and closed sources, and includes several privileged feeds which are not available elsewhere.

44. Early Warning filters millions of events that the NCSC receives every day and, using the IP and domain names organisations or individuals provide, correlates those which are relevant to their organisation into daily notifications for their nominated contacts via the Early Warning portal.

Insurance

45. The cross-Government ransomware sprint in 2021 identified cyber insurance as a potential market influence to encourage good cyber behaviour in their customers.

46. A sophisticated cyber insurance market could help tackle ransomware through risk-based pricing, which could incentivise better cyber security practices. This could be through a range of market influencers, stimulating demand for greater investment in cybersecurity. Alongside cyber insurance, organisations should prioritise and invest in cyber security and cyber resilience.

47. However, the UK cyber insurance market is underdeveloped: the Cyber Security Breaches Survey[30] states that whilst 43% of businesses have an insurance policy that covers cyber risks, only 5% have a specific cyber standalone policy (which are generally clearer on their scope). Both Industry and Government have identified data scarcity as a key barrier to market growth. Without this data, insurers will have less incentive to enter the market or will price risk too highly which limits policy sales. To rectify this, HM Treasury (HMT) has worked closely with the Information Commissioner's Office (ICO) to build a case for the greater release of cyber breach data and was pleased to see the ICO release, in accordance with public interest, an anonymised set of the data it holds. This data will help insurers to better price risk and develop their cyber insurance offerings.

48. The Cyber Security Breaches Survey 2022 noted some difficulty with obtaining insurance: *"in previous years organisations have mentioned protection against ransomware and assistance with payments as a key reason for getting insurance. However, this year it was mentioned that this had become more difficult with insurance companies raising premiums or not being able to cover ransoms at all."*

49. Alongside HMT's work on insurance, the NCSC lead an Insurance Trust Group, with members from various Government Departments, including the Home Office, HMT and DCMS. The role of the Trust Group is to keep members informed of relevant policy proposals and provide opportunity for feedback on government initiatives such as cyber security and reporting levels.

[30] Cyber security breaches survey 2022 - GOV.UK (www.gov.uk)

50. NCA engagement with the cyber insurance sector is also fast developing. Cyber insurers' visibility to the threat makes them an attractive partner to engage with as they hold considerable information on ransomware incidents across sectors and business sizes, many of which are unreported to law enforcement and may not appear on data leak sites.

The effectiveness of the response to ransomware by Government, law enforcement agencies and other UK state actors, including key operational challenges and ministerial oversight

51. Ransomware is a top priority for Government, given its severity in threat level. However, the levers and mechanisms that we have to reduce the impact of ransomware and combat the threat it poses sit across HMG. Therefore, oversight and decision-making sits with Ministers across government, and all recommendations and updates that Ministers receive are over seen by the Senior Ransomware Steering Group (SRSG). The SRSG brings together cross-HMG policy, intelligence and law enforcement partners to provide oversight to this work. It facilitates the sharing of learning and evidence to collectively drive activity to counter the ransomware threat. The SRSG is led by the Home Office's Director for State Threats and Cyber, and support is provided by the Home Office.

52. The SRSG reviewed proposed future ransomware policy work and is collectively focused on delivering the four key outcomes developed as part of the 2021 ransomware sprint. The four key outcomes are as follows:
    a) The vulnerability of UK targets to ransomware attack is reduced
    b) The impact of ransomware attacks on victims is reduced
    c) The incentives for attackers to use ransomware are reduced
    d) The capabilities of ransomware attackers are reduced

53. Previous cross-HMG work was completed under the ransomware sprint which explored a range of policy options, including reporting levels, engagement with the insurance industry, decreasing payments to ransomware actors, applying cyber sanctions to ransomware actors, consideration of future application of cyber sanctions to ransomware actors, and increasing our international influence.

54. Following the UK's exit from the EU, the Cyber (Sanctions) (EU Exit) Regulations 2020 were introduced under the Sanctions and Anti-Money Laundering Act 2018. Cyber sanctions are a key tool for responding to and deterring cyber-attacks, including ransomware. Along with public attribution of specific activity, they impose meaningful cost and send a signal that malicious cyber activity has consequences[31]. We continue to use sanctions – in conjunction with our allies – to impose costs on those that conduct malicious cyber activity against us or threaten the peaceful use of the internet.

[31] The regulations also make it an offence, subject to certain exceptions, for anyone to make funds available to a person designated under the cyber sanction schemes.

55. Ransomware is a Computer Misuse Act (CMA) offence (amongst other offences), and the Home Secretary announced a review of the Computer Misuse Act on 11 May 2021. The first step in the review was a public Call for Information, to seek the views of those with an interest in the Act on how it – and the powers available to law enforcement agencies to investigate the CMA offences – could be enhanced. The Home Office received a number of responses and is considering these as part of the overall review.

56. There is also wider work being undertaken across HMG and with the private sector to reduce the flow of money to ransomware actors through forthcoming strategy. Tackling money laundering requires a co-ordinated, cross-system response to disrupt and dismantle the criminal business models that cause significant harm to victims and undermine our democracy and legitimate economic growth. New legislation is helping to respond to the changing threat, as the proceeds of crime are increasingly held in the form of cryptoassets. The new Economic Crime and Corporate Transparency Bill, currently in Parliament, aims to strengthen the UK's fight against economic crime through the introduction of new criminal and civil proposals, which include:

a) Removing the need to arrest a person before cryptoassets can be seized
b) Aligning provisions for recovery of cryptoassets with other types of property

57. HMT and the Financial Conduct Authority (FCA) are also working to disrupt the ransomware business model and reduce actors' ability to access finance. This includes establishing a Cryptoassets Taskforce in 2018, consisting of HM Treasury, the Bank of England and the Financial Conduct Authority. The Taskforce's objectives include exploring the impact of cryptoassets, the potential benefits and challenges of Distributed Ledger Technology (DLT) in financial services; as well as continually assessing what, if any, regulation is required in response. This culminated in the publication of the UK regulatory approach to cryptoassets[32], including the intent to legislate and bring stablecoins within the regulatory perimeter, alongside legislating to create a DLT financial market infrastructures sandbox.

58. This means creating a robust regulatory environment in which firms can innovate, while crucially maintaining high regulatory standards so that people can use new technologies both reliably and safely. This is essential for continuing confidence in the financial system more broadly.

59. Cryptoassets can be moved across borders quickly, and it is therefore important for the UK to work collaboratively with our international partners. Further detail on our international work can be found at paragraph 75.

[32] UK regulatory approach to cryptoassets, stablecoins and DLT in financial markets

Potential reforms that might enhance the UK's resilience to ransomware, reduce the economic and societal damage that it causes, and/or support the law enforcement response.

60. Bolstering the UK's cyber resilience is critical to tackling the ransomware threat, as improving our ability to prevent and respond to cyber attacks will reduce the number of successful attacks and their impact on the UK. The National Cyber Strategy sets out to enhance UK cyber resilience through three key objectives:

a) Improving the understanding of cyber risk.
b) Preventing and resisting attacks by improving management of risk within UK organisations.
c) Strengthening the UK's resilience to prepare for, respond to and recover from attacks.

61. The NCSC plays a central role in supporting work on cyber resilience and directly reducing the ransomware threat. As part of their work, they have launched a new ransomware portal[33] with refreshed advice and guidance, including practical resources to help users prevent, report, respond to and recover from attacks.

62. Alongside this, the NCSC continues to provide advice and guidance on cyber resilience. This guidance includes: making sure victims know how to recover after an incident and the importance of backups[34], how to defend organisations against malware or ransomware attack[35], guidance for organisations on how to choose, configure and use devices securely[36], recovering a hacked account[37], recovering an infected device[38], how to assess and gain confidence in supply chain cyber security[39], and Joint Venture in the Construction Sector and Information Security[40]. This is not an exhaustive list but is illustrative of the types of guidance, advice and blogs NCSC publish on increasing cyber resilience.

63. Our aim for cyber resilience for businesses, organisations and citizens is to set clear expectations underpinned by the right framework of incentives, support and regulation to enable improvement and transfer the burden of cyber security risk away from end users and towards those best placed to manage it. We are helping citizens understand the basic steps they can take through the Cyber Aware campaign, which has had 1.2m views in two-and-a-half years[41].

---

[33] A guide to ransomware - NCSC.GOV.UK
[34] Backing up your data - NCSC.GOV.UK
[35] Mitigating malware and ransomware attacks - NCSC.GOV.UK
[36] Logging and protective monitoring - NCSC.GOV.UK
[37] Recovering a hacked account - NCSC.GOV.UK
[38] How to recover an infected device - NCSC.GOV.UK
[39] How to assess and gain confidence in your supply chain... - NCSC.GOV.UK
[40] Joint Ventures in the Construction Sector (ncsc.gov.uk)
[41] Cyber Security Breaches Survey 2021 Education Annex – DCMS.GOV.UK

64. Earlier this year HMG published the Cyber Security Incentives and Regulation Review[42], which details the progress made in improving cyber resilience between 2016 and 2021, and provides evidence and analysis as to why further action needs to be taken to ensure we are effectively managing cyber risk in the UK, embedding cyber security as a core part of good business. As part of reforms to audit and corporate governance, we are taking forward improvements to give investors and shareholders better information on resilience risks, specifically including consideration of cyber risks (which should include the threat from ransomware). HMG has committed to ensure that technical advice, self-help tools and assured products and services continually improve and are readily accessible to the people and organisations that need to use them. This will ensure that the advice and tools provided keep up to date with the ransomware threat, and what action should be taken to mitigate it.

65. HMG is also scaling up work to make the internet safer, preventing ransomware attacks, and building in basic protections by default. The UK is the first country to mandate minimum security standards for consumer connected ("smart") products through the Product Security & Telecommunications Infrastructure Bill[43]. DCMS is publishing a world-first Code of Practice to secure apps and app stores by setting baseline security and privacy requirements to protect users. They are engaging local authorities, industry and internationally to ensure connected places ('smart cities') technology is adopted in a way that protects human rights and is secure and sustainable. Alongside this there are teams across HMG that focus on horizon scanning for science and technology developments including those most vital to the UK cyber sector in order to better understand the associated risks and opportunities.

66. DCMS leads the building of domestic capability to improve cyber resilience by strengthening our industrial and skills base. There was a shortfall of c.14,100 people in the UK cyber security workforce in 2021[44], and 51% of businesses lack basic technical cyber skills[45]. DCMS provides targeted regional support to cyber businesses at every stage of development. This year, they have also provided a funding of £8m for programmes to improve skills among school children, youth, and adults. They have also set up the UK Cyber Security Council to support professional development of those working in or aspiring to work in cyber security professions.

67. Alongside ensuring that there is good cyber resilience across the economy, HMG has sought to bolster the capabilities of the public sector and HMG itself. Aligning with the work referenced in paragraph 36, HMG launched the first ever Government Cyber Security Strategy (GCSS) in January 2022. It sets out how we will build and maintain our cyber defences; by building greater cyber resilience across all government

[42] 2022 cyber security incentives and regulation review – DCMS.GOV.UK
[43] Product Security and Telecommunications Infrastructure Bill
[44] Cyber security skills in the labour market 2022
[45] Cyber security skills in the labour market 2022

organisations, and working together to 'defend as one' - exerting a defensive force greater than the sum of our parts. The Strategy sets a clear target for government's most critical functions to be appropriately resilient by 2025, with all government organisations being resilient to known vulnerabilities and common attack methods by 2030[46].

68. The Covid-19 pandemic has highlighted the reliance we now place on accessing essential services digitally which have allowed us to function as normally as we can. The GCSS recognises that there is an increase in the number and severity of cyber attacks, and that cyber resilience is a cost-effective and impactful lever against the threat. We will also ensure that incident management teams have the requisite expertise, capacity and capabilities to respond to the full range of evolving incident types, including ransomware.

Incident management

69. In the National Cyber Strategy we committed to making our response to nationally significant cyber incidents even more effective, and we are taking steps to ensure that lessons identified are used to improve our policies and processes.

70. HMG provides support to victims of ransomware attacks at both an individual and organisational level and provides national coordination of incident responses when required. For the most critical cyber incidents, the Cabinet Office works closely with the NCSC and law enforcement, in order to coordinate the cross-government response, up to and including COBR activation. The key objective of this response is to manage impacts, support continued service provision and recovery.

71. To deliver the law enforcement element and ensure a timely and agile response to urgent, complex, or serious investigations, including live cyber attacks, the NCA established the National Cyber Crime Unit Triage, Incident Coordination and Tasking Team (TICAT). TICAT has been pivotal in the operational response, acting as the gateway into the NCCU for intelligence referrals, reported live incidents, and providing a tasking mechanism across the National Cyber Crime Network. In addition, TICAT has responded to the changing threat and adapted to ensure it can deliver effective incident response and victim support to live cyber incidents. This is demonstrated by an increase in the live interventions and mitigations that TICAT is now able to deliver. TICAT's incident response mechanism is supported by NCCU's upstream investigations which identify the modus operandi of High End of High Harm (HEHH) cyber-OCGs, thereby enhancing NCCU's understanding and enabling better victim support. NCCU TICAT is constantly improving its engagement with victims and any advice offered, which may assist mitigation of the incident itself and remediation of victim systems.

Law enforcement response

[46] Government Cyber Security Strategy: 2022 to 2030 - GOV.UK

72. The reality is that criminal justice outcomes against High End of High Harm (HHEH) offenders are often unrealistic and as such the National Crime Agency's National Cyber Crime Unit (NCCU) has been required to develop a range of alternative disruption methods as part of a 4P (Prepare, Prevent, Pursue and Protect) response. Wherever possible the NCCU works collaboratively with national and international partners to disrupt HEHH cyber-offenders.

73. A recent initiative has established the Ransomware Working Group across the National Cyber Crime Network (NCCN) to share best practice, expertise and experiences across the network to enhance the response. This is welcome as a forum to bring the NCCN community together, but for the moment is focused on reactive as opposed to proactive activity.

74. The NCCU is currently the leader of the Five Eyes Cyber Crime Working Group (CCWG) and International Cyber Crime Operational Group (ICCOG) of Five Eyes and European partners. These fora bring together our most important operational partners from across

The scope for International Cooperation to combat the global ransomware threat more effectively, including on crypto-currency regulation.

75. The UK is a world leader in cyber security and the NCSC is widely regarded as a source of international best practice. The Government regularly shares its approach to cyber security, as outlined in the National Cyber Strategy, with international partners. Cabinet Office, NCSC, the Home Office and other government departments are frequently asked to brief other countries on our national approach to ransomware.

76. As a responsible cyber power, the UK is at the forefront of responding to cyber threats, imposing costs on states involved in malicious cyber activity and cybercriminals, shaping the governance of cyberspace and building our allies' resilience and willingness to respond. The National Cyber Strategy sets out the role the UK will play as a 'democratic, responsible cyber power' and our commitment to working with allies and international partners to promote a free, open, peaceful and secure cyberspace. As cyberspace is borderless, any approaches need to be international. The UK shapes the global conversation at multilateral forums such as the United Nations, International Telecoms Union, North Atlantic Treaty Organisation, European Union, G7, Organisation for Security and Co-operation in Europe (OECD), the Financial Action Task Force and bilaterally around the world to respond to and deter malicious cyber activity.

77. The UK is active in the international combatting-ransomware sphere: we lead the G7 ransomware work strand in 2022, are a proactive member of the Ottawa 5 Ransomware Working Group and co-chair the Countering Illicit Finance Working Group within the Counter Ransomware Initiative (CRI).

Counter Ransomware Initiative

78. The US-led Counter Ransomware Initiative (CRI) was announced by US President Joe Biden in October 2021. This initiative brings together approximately thirty-seven countries to strengthen cooperation against ransomware and tackle misuse of cryptocurrencies. Anne Neuberger, Deputy National Security Advisor at the White House leads the CRI.

79. As the CRI enters its second year, it is changing structure to a task force model under the International Countering Ransomware Task Force (ICRTF). The UK will continue our leadership role under the policy strand, jointly with Singapore, and will facilitate a number of projects, including on barriers to data sharing; insurance; and options to reduce payments.

80. To facilitate this, the UK has been in close communication with other members around priority focus areas, including actively utilising the newly established platform for information-sharing between the public and private sectors on actors and tradecraft, and rolling out a capacity-building tool on how to develop national and local public-private partnerships to combat ransomware.

Countering Illicit Finance

81. The UK and Singapore co-chair the Countering Illicit Finance Working Group (CIFWG) within the CRI, with a focus on improving the policy response to illicit finance aspects of countering ransomware, through both law enforcement and financial regulation policy engagement. Predominantly, this relates to cryptoassets, as the primary payment method for ransoms. The working group has so far also focused on improving the reporting of ransomware attacks, improving the depth and consistency of anti-money laundering supervision of cryptoasset exchanges and wallet providers, the implementation of anti-money laundering standards for cryptoasset businesses and engaging with the insurance sector.

Increasing Resilience

82. As part of the CRI's resilience focus, in September 2022, India and the UK co-led an international cyber exercise to test the responses of partners to a ransomware attack on the electricity distribution/energy sector. This was funded and facilitated by FCDO's Cyber Policy Department which co-ordinated the delivery of this exercise through BAE Systems. The exercise was the first deliverable of the India-UK Enhanced Cyber Partnership, built on the UK-India 2030 Roadmap. Sixteen countries participated in person or virtually (India, UK, Brazil, Estonia, Ireland, Italy, Lithuania, Mexico, Netherlands, Poland, Romania, Spain, Sweden, Switzerland, Ukraine and the USA). The exercise included policy, operational, law enforcement and energy sector experts from each government.

Conflict, Stability and Security Fund

83. Besides the CRI, the FCDO lead the Conflict, Stability and Security Fund (CSSF) Cyber Portfolio (worth c£90m over the SR period 2022-2025), which seeks to support priority partner countries to improve their cyber security resilience, including building their capability to tackle cyber-dependent crimes like ransomware. Recent successes include:

a) Partnership with the United Nations Office on Drugs and Crime (UNODC) and the Commonwealth Secretariat to strengthen cyber crime legislation, enforcement and international co-operation (including a recent conference on addressing cybercrime in Asia). Over 1,500 officials were trained in 2021-22.
b) Partnership with Interpol to establish their Africa counter-cyber crime desk, which runs cross-border law enforcement operations and awareness-raising campaigns. This has resulted in arrests of 12 members of a Nigerian cyber crime network since the project started in 2021.
c) Training Nigerian and South African law enforcement in key counter-cyber crime techniques.
d) Building broader resilience to cyber threats, including developing cyber security regulatory frameworks for Indonesian finance and healthcare systems; running national cyber threat response exercises in India, Sri Lanka, Colombia, South Africa; supporting Nigeria, Botswana, Zambia and Association of Southeast Asian (ASEAN) members to assess cyber threats to critical national infrastructure; improving user- and SME-level awareness of basic cyber safety through campaigns in Nigeria and South Africa.

84. We also promote the Budapest Convention as the leading international agreement on tackling cybercrime and an effective template for international cooperation. This was initially a Russian proposal which we and our allies resisted. However, on 27 December 2019 the UN General Assembly (UNGA) adopted a Russian resolution in favour of developing a new international treaty on cybercrime. The UK is actively participating in the negotiations, alongside our allies.

International law enforcement cooperation

85. HMG has mature and productive information-sharing relationships with its overseas partners. This information-sharing is underpinned by close relationships between HMG's operational partners (such as the NCSC and the NCA) and those of its overseas equivalents. The NCA currently chairs the Five Eyes Law Enforcement Group Cyber Crime Working Group (FELEG CCWG), and the International Cyber Crime Operations Group (ICCOG), two multilateral forums that bring together international law enforcement partners to tackle the cyber crime threat, with a focus on ransomware. Where there have been significant incidents (including ransomware) involving our overseas partners the UK's operational partners will support, co-operate and work with their counterparts to ensure that they have as much information as possible to manage and contain the incident.

86. For example, as part of their operations, the NCA uses a variety of tactics and niche capabilities to identify and disrupt offenders. This includes monitoring their travel, dismantling wider criminal networks (including those developing and deploying ransomware), tackling criminal infrastructure and marketplaces, and targeting their financial flows.

87. A key example of this is the NCA's work with US partners to tackle Evil Corp. The NCA launched a joint operation with the FBI and the Office of Foreign Assets Control (OFAC) against Evil Corp, a Russian cyber crime group, in 2019. They were dubbed the world's most harmful cyber crime group having created and deployed malware causing financial losses totalling hundreds of millions of pounds in the UK alone. The head of the group and another member were indicted in the US and made subject to international sanctions. Maksim Yakubets, a leading member of Evil Corp, was sanctioned by OFAC for connections to the FSB. The sanctions and indictments have forced Evil Corp into repeated rebranding and recoding of their ransomware strains to avoid these interventions. Visibility and awareness of Evil Corp has increased substantially since the public attribution. While they continue to be able to commit this criminality due to the lack of Russian state action against them, their need to continually change is nonetheless an additional cost they must bear which previously was not the case.

Lessons that could be learned from other countries' approaches and responses to ransomware.

88. As well as sharing our own best practice, the Government also frequently draws upon the approaches and expertise of other countries in its cyber security work. This is particularly the case in responding to ransomware incidents and learning from other countries who have experienced significant ransomware attacks. There have been a number of significant ransomware incidents internationally in recent years that the UK has considered closely and taken lessons from, such as the US response to the Colonial Pipeline ransomware attack in May 2021. Alongside this, the UK continually reviews lessons learnt from other international partners on their approaches to tackling ransomware.

89. Through the Ransomware Action Plan, the Australian Government is looking to pursue legislative reforms including specific mandatory ransomware incident reporting to the Australian Government, introducing a standalone offence for all forms of cyber extortion and aggravated offence for cyber criminals targeting CNI, and modernising legislation to hold cyber criminals to account through law enforcement tracking, and seizing or freezing of assets.

90. The USA facilitated the Counter Ransomware Initiative (CRI) and has called on its own private sector (who own and operate the majority of USA CNI) to help act on ransomware and modernise their cyber defences. This includes working with industry

to improve current and emerging standards, practices and technical approaches. In early 2022, the US Senate passed legislation that required organisations working in CNI to report hacks and ransomware attacks. Targeted organisations are also required to preserve data and provide updates if new information emerges.

91. The European Union attended the CRI summit in 2022 and recognises that ransomware is a high EU priority. The European Union Agency for Cybersecurity, established in 2004, is exploring ways to improve the reporting of incidents and have revised the Network and Information Security Directive (NIS 2). This EU-wide legislation will set the baseline for cybersecurity risk management and reporting obligations to help further Member States' cybersecurity capabilities. The directive will establish the European Cyber Crises Liaison Organisation Network (EU-CyCLONe) to support the management of large-scale cybersecurity incidents.

92. Through the CRI we have been able to further support the sharing of lessons learned and discuss opportunities for strengthening our resilience and capabilities to disrupt ransomware actors and bring them to justice. The work of the CRI supports the implementation of the endorsed UN framework for responsible state behaviour in cyberspace, specifically the voluntary norm that States should cooperate "to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats."

93. Following major incident responses, the government routinely reviews its response and identifies actionable steps it can take to further improve the effectiveness of its incident response capabilities and processes. We will continue to share crisis management experience with international partners and identify best practice to enhance our preparedness and processes.

16 December 2022