Home Office

Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting

Government response

Published on: 22 July 2025

Contents

Contents 1

Introduction and contact details 4
- Introduction 4
- Contact details 4
- Complaints or comments 4
- Freedom of information 4

Executive Summary 5
- Overview 5
- Consultation outcomes 6
- Proposal 1 feedback 6
- Proposal 2 feedback 7
- Proposal 3 feedback 8
- Cross-cutting themes 8
  - Scope of the proposals 8
  - Penalties 8
  - Guidance and support 9
  - Cyber awareness and resilience 9

Methodology 10

Summary of responses 12
- Respondent characteristics 12

Proposal 1 14
- Proposal summary 14
- Analysis summary 14
  - Question 10 14
  - Questions 11 and 12 16
  - Question 13 18
  - Question 14 19
  - Question 15 21
  - Question 16 22
  - Question 17 24
  - Question 18 25
- Government policy response 26

Proposal 2 28
Proposal summary 28
Analysis summary 28
Question 19 28
Questions 20 and 21 30
Question 22 32
Question 23 34
Question 24 35
Question 25 37
Question 26 38
Question 27 39
Question 28 39
Government policy response 40
Proposal 3 42
Proposal summary 42
Analysis summary 42
Question 29 42
Questions 30 and 31 44
Question 32 46
Question 33 48
Question 34 49
Question 35 50
Question 36 52
Question 37 53
Question 38 53
Question 39 55
Question 40 56
Government policy response 56
Additional Comments 59
Analysis summary 59
Question 41 59
Question 42 60
Question 43 60
Impact Assessment, Equalities and Welsh Language 61
Equality Impact Assessment 61
Section 1 - Name and outline of policy proposal, guidance, or operational activity 61

Section 2 - Summary of the evidence considered in demonstrating due regard to the Public-Sector Equality Duty (PSED). 61

Section 3 - Consideration of duty 62

Section 4 - Community Considerations 65

Section 5 - Summary of foreseeable impacts of policy proposal, guidance or operational activity on people who share protected characteristics 65

Section 6 - In light of the overall policy objective, are there any ways to avoid or mitigate any of the negative impacts that you have identified above? 67

Section 7 – Review date: 67

Section 8 - Declaration 67

Equalities 68

Welsh Language Impact Test 68

Consultation principles 69

Annex A – Consultation Questions 70

Introduction and contact details

Introduction

The Government consultation on proposed ransomware legislative measures was open for 12 weeks (from 14th January 2025 to 8th April 2025). The consultation closed before the recent cyber attacks affecting several organisations in the retail sector.

Contact details

This document sets out the Government's response to the public consultation: Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting

Comments on the Government's response can be sent to:

Ransomware Legislative Proposals Consultation

Home Office
5th Floor
Peel Building
2 Marsham Street London
SW1P 4DF

or

ransomwareconsultation@homeoffice.gov.uk

Alternative format versions of this publication can be requested from the above address.

Complaints or comments

If you have any complaints or comments about the consultation process you should contact the Cyber Policy Unit at the above address.

Freedom of information

Information provided during this consultation, including personal information, may be published or disclosed in accordance with access to information regimes, primarily the Freedom of Information Act 2000 (FOIA) and the Data Protection Act 2018 (DPA).

The Home Office will process your personal data in accordance with the DPA and, in the majority of circumstances, this will mean that your personal data will not be disclosed to third parties. This consultation follows the UK Government's consultation principles.

Executive Summary

Overview

In the UK, ransomware is considered the greatest of all serious and organised cyber crime threats and is deemed as a risk to the UK's national security by the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC)[1].

In January 2025, the Home Office launched a consultation on a package of proposals to reduce the threat that ransomware poses to the UK economy. Alongside the consultation, significant stakeholder engagement took place. The three proposals that were consulted on are:

1. A targeted ban on ransomware payments for owners and operators of regulated-critical national infrastructure and the public sector.
2. A ransomware payment prevention regime.
3. A mandatory incident reporting regime.

If progressed, this package of proposals would be the first specific measures in UK law to counter ransomware.

The proposals are a targeted and proportionate response to the most significant cyber national security threat facing the UK. They are part of a wider, holistic approach to cyber threat and are consistent with, and complementary to, the resilience measures undertaken by the NCSC, the Cabinet Office and the Department for Science, Innovation and Technology. The proposals intentionally do not repeat any of this long-established work. Feedback that includes resilience measures will be anonymously shared with these departments.

The Home Office continues to collaborate with these departments to increase resilience, as any overall increase in resilience helps to reduce the risk of ransomware. The consultation proposals demonstrate bespoke, targeted action to mitigate specific ransomware-related behaviours and threats and break the payment cycle/business model of the criminal gangs.

The overall response to the proposals has been positive. There were high levels of engagement and thoughtful commentary throughout. The Government will continue to reflect on and take into account the helpful feedback when developing these measures.

[1] The National Crime Agency describes ransomware as one of the most harmful cyber threats due to the significant financial losses incurred; the threatened theft of intellectual property, sensitive commercial data, or customer Personally Identifiable Information (PII); the disruption of service caused by attacks; and the reputational harm that can result.

Consultation outcomes

The Government's response to the consultation offers an overview of the responses, key findings and sets out the next steps for policy development. There have been 273 responses, of which 233 were via the online survey or followed the survey format. A further 40 responses took other forms, such as emails or written prose. Alongside formal responses, the Government held 36 events to encourage engagement in the consultation process. This feedback has also been considered but is not included in the overview of responses.

Overall feedback from respondents was positive and constructive. The Government intends to continue to develop these measures in collaboration with industry, and guidance and other supporting and clarifying documents will be made available.

Proposal 1 feedback

A targeted ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of critical national infrastructure (that are regulated, or that have competent authorities).

Overall, nearly three quarters (72%) of respondents agreed that HMG should implement a targeted ban on ransomware payments for CNI owners and operators and the public sector, including local government. Less than a quarter (23%) of respondents disagreed.

Just over two thirds of respondents (68%) thought that a targeted ban will be effective in reducing the amount of money flowing to ransomware criminals and thus reducing their income. Six in ten (60%) respondents also thought that a targeted ban will be effective in deterring cyber criminals from attacking those organisations subject to the ban.

There were mixed views on any exemptions to the ban, and on widening the ban to CNI and public sector supply chains.

Whilst all respondents were welcome to respond to this proposal, it was specifically seeking views of those who operate within or consider themselves as CNI and/or the public sector. CNI/public sector[2] respondents showed slightly higher levels of agreement (82%) than those who did not respond as CNI/public sector organisations (69%). A slightly higher proportion of CNI thought this proposal would be effective, compared to individuals, at reducing the amount of money flowing to ransomware criminals (74% for CNI, compared to 70% for individuals) and deterring cyber criminals (79% for CNI, compared to 68% for individuals).

[2] This category includes, CNI, local government, central government/civil service, and other public sector/public body.

Proposal 2 feedback

A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.

There were mixed views on a new ransomware payment prevention regime, but of the measures presented, *'Measure 1: an economy-wide payment prevention regime for all organisations and individuals not covered by the targeted ban'* had marginally more support (47% net agreement) than the other measures. Feedback expressed through the qualitative aspects of the survey outlined that this approach would have arguably fewer issues than Measures 2 - 4[3]. However, it is at odds with those who may feel that an economy-wide approach is disproportionate.

For the other Measures 2-4, a larger proportion of respondents disagreed with implementing these measures (48 – 53% levels of net disagreement). Respondents raised issues on a threshold-based approach to a payment prevention regime, including the risk of criminals shifting their methods or targets to those not covered by the regime.

Views expressed in the qualitative responses provided insight into some of the risks that need to be considered ahead of implementation. This included outlining that a threshold approach would have an increased potential for displacing attacks to those not covered; and would likely create more loopholes or shape business practices to avoid falling within any stated threshold. A possible inference of these quantitative and qualitative responses suggests there was mixed opinion across respondents on how to best implement a ransomware payment prevention regime, rather than disagreement with implementing the proposal in principle.

There were also split views on how effective proposed measures for the ransomware payment prevention regime would be, including law enforcement's ability to intervene and investigate the threat of ransomware. However, Measure 1 had the highest proportion of respondents who thought it would be 'effective' for both reducing ransomware payments (27%) and increasing ability of law enforcement agencies to intervene and investigate ransomware actors (22%).

Recurring qualitative feedback included wanting clarity on the process, including timings (e.g. how long would it take for the Government to decide whether to block a payment), and concerns that if any regime is not economy-wide, it could displace attacks onto those sectors not included.

[3] Measure 2: threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1. Measure 3: Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals. Measure 4: Threshold based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.

Proposal 3 feedback

A ransomware incident reporting regime that could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

Responses show agreement that a new mandatory reporting regime should be introduced, with all new measures viewed more favourably than Measure 1, which proposed the continuation of the existing voluntary ransomware incident reporting regime.

'Measure 2: an economy-wide mandatory reporting requirement for all organisations and individuals' had the highest proportion of agreement to implement (63% net agreement). In comparison, less than half (41% net agreement) agreed with continuing the current voluntary reporting system.

Around three quarters of respondents thought that this economy-wide measure would be effective in increasing the Government's ability to understand the ransomware threat to the UK (79% net effective), and effective in increasing the Government's ability to tackle and respond to the ransomware threat in the UK (74% net effective).

Recurring feedback included discussions around whether further threshold requirements for reporting would be suitable, such as based on an organisation's annual turnover, or the number of employees they may have.

Respondents also highlighted whether individuals should be considered under the mandatory ban, as well as organisations, noting the additional resource implications of a new reporting requirement and whether fulfilling obligations for an individual was deemed reasonable. Views were also expressed on the impact a reporting regime will have on organisations' resources, as many are already subject to various existing reporting requirements.

Cross-cutting themes

Scope of the proposals

Responses to all three proposals requested clarification around the scope of the individual measures. For the proposed public sector and CNI payments ban, responses reflected our question of whether this would include supply chains, how CNI operators would be defined, and considerations around extraterritorial powers. For the ransomware payment prevention regime and mandatory reporting, respondents queried whether these measures would apply to both individuals and organisations. Further responses asked whether there should be threshold requirements for compliance measures based on an organisation's annual turnover, the size of ransom demanded, or number of employees.

Penalties

A key theme identified across responses to all proposals was the role of penalties. Respondents agreed with the use of penalties across all proposals. However, concern was

expressed over the proportionality of any penalties, whether criminal or civil penalties would be suitable, whether penalties should be tailored, and that consideration should be taken to avoid criminalising or revictimising victims.

Guidance and support

Another cross-cutting theme was the need for any guidance and support to be tailored, including sector-specific advice on how proposals should be implemented and making these resources clear and accessible. Across all three proposals, the need for Government and Law Enforcement victim support in the event of an attack was also put forward by respondents.

Cyber awareness and resilience

Across all the proposals, respondents also commented on the need to improve cyber awareness and resilience regardless of the proposals suggested. This included updating IT systems, improving incident response mechanisms, and having robust backup and restoration processes.

Methodology

The consultation was open for 12 weeks (from 14th January 2025 to 8th April 2025). Respondents could respond via an online survey or email.

The survey comprised of 43 questions, including 9 demographic/characteristic questions and 32 main survey questions. All questions were multiple-choice and 23 of the questions had additional free text boxes for optional further information.

There were two further questions under a 'Call for Evidence', seeking information and data to further understand the ransomware threat.

The results are representative of the individuals and organisations who completed the consultation survey, either via the online survey link or an emailed version via the consultation inbox. Other longer form responses received have been read and summarised into relevant sections.

The Home Office publicised the consultation and encouraged engagement through several means, including industry events, sharing through government department networks, social media and media activity. However, public consultations are, by their nature, self-selecting and results cannot be viewed as fully representative of the general population, or of all organisations.

This document contains responses to closed questions. Notes on the quantitative data and analysis:

- Percentages presented in this report may not sum to 100% due to rounding
- Not all respondents answered every question, resulting in varying base numbers between questions
- Graphs and percentages reflect the analysis of the 233 respondents who completed the online survey or sent an emailed version via the consultation inbox
- Response categories for questions on agreement and effectiveness have been combined to provide a 'net' percentage, for example 'strongly agree' + 'tend to agree' to give a net agreement percentage. Where this is not the case and an individual category is referenced, this has been specified.

Common themes from open-ended questions are also included in this report, based on thematic coding. For these open-ended questions, there was a manual coding process. Responses to open-ended questions were read and assigned relevant codes, and groups of similar codes have been grouped together into overarching categories. Subjectivity or bias was minimised by carrying out additional quality assurance checks, where a separate analyst recoded a percentage of the codes and reviewed the categories created to ensure

accuracy and reliability. Examples of open-ended question responses are given where relevant and quotes have been selected to illustrate key themes from the analysis. They are not used to show the proportion of respondents who have responded this way.

Summary of responses

A total of 233 survey style responses to the consultation were received, of which 10 were submitted in an emailed version via the consultation inbox. An additional 40 responses were received that were not in the survey style. This included emails and long form prose style responses. These prose responses were primarily from financial, insurance, and membership bodies. They are not included in the quantitative survey analysis, but have been read alongside the survey qualitative responses, and any additional key themes have been identified where relevant.

Figure 1: Breakdown of formal consultation respondents

Response Format	Number of Responses
Survey Style	
Online Survey	223
Emailed version of the survey	10
Non-Survey Responses	
Prose responses	26
Additional emails and miscellaneous responses	14
Total	**273**

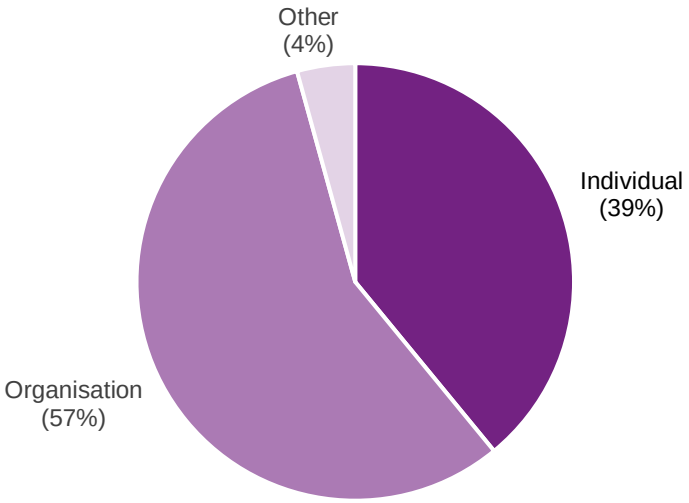
Alongside formal responses, the Government encouraged engagement with the consultation process through 36 engagement events. These events included Q&A sessions, presentations, and attending industry events, and aimed to address a variety of sectors, including industry, insurance, CNI, academia, and finance. This feedback has also been considered in the consultation process but is not included in the overview of responses. These engagements have led to ongoing discussions with key stakeholders.

Respondent characteristics

Questions 1 – 9 were demographic and characteristic questions, asked to help us understand the population of respondents to the consultation. These also allow us to segment some of the question responses to provide more specific insights.

Of the 233 survey respondents, 57% responded on behalf of organisations and 39% responded as individuals. The ‘Other’ category made up 4% of the respondents. Respondents for the ‘Other’ category were able to define themselves and this category included, for example, community networks or cyber security experts.

Figure 2: Breakdown of respondents by individual and organisation



Q. *Are you responding to this survey as an individual or as a representative of an organisation?* ***Base*** *= All (n=233)*

There was also a spread in the size of organisations that responded. However, over half had 250+ people working for them (58%) and nearly half (48%) had an annual turnover of £50,000,000 or more.

Proposal 1

Proposal summary

A targeted ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of critical national infrastructure (that are regulated, or that have competent authorities).

A targeted ban on ransomware payments for public sector bodies, local government and CNI owners and operators would mean organisations considered in scope would be unable to make a payment to a threat actor in the event of a ransomware attack. Ransomware threat actors operate via financial extortion. A payment ban aims to remove the financial incentives of targeting these organisations, reduce threat actors' revenue streams and capabilities (by limiting their ability to reinvest profits), and disincentivise attacks on UK organisations by making them financially unattractive targets.

The proposed ban would go beyond the current UK Government position, that government departments should not use taxpayer money to pay ransoms. By further restricting ransomware payments, the Government would seek to affirm a non-payment position across public sector bodies, local government and CNI owners and operators.

Analysis summary

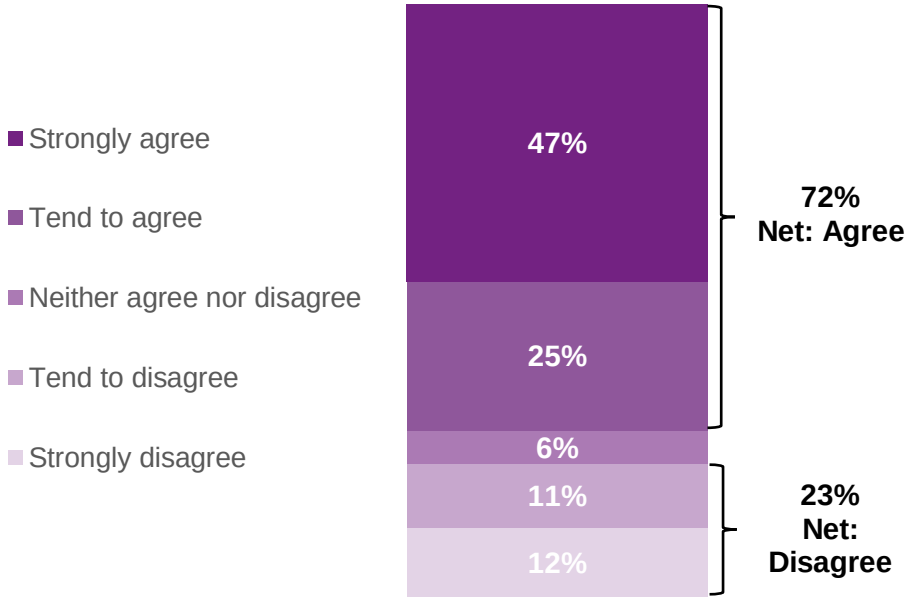
Questions on Proposal 1 were largely directed at those CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, but responses were also welcome from others with an interest in these sectors.

Question 10

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

Nearly three quarters (72%) of respondents agreed that HMG should implement a targeted ban on ransomware payments for CNI owners and operators and the public sector, including local government. Less than a quarter (23%) of respondents disagreed.

Figure 3: Agreement levels for implementing a targeted ban on ransomware payments for CNI owners and operators and the public sector



Q10. *To what extent do you agree, or disagree, that HMG should implement a targeted ban on ransomware payments for CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government?* ***Base*** *= all respondents (n=231)*

There were differences among sub-groups in agreement that HMG should implement the targeted ban:

- Individual respondents had a higher level of agreement (81%) than organisations (65%)
- CNI/public sector[4] respondents showed slightly higher levels of agreement (82%) than those who did not respond as CNI/public sector organisations (69%)

A range of views were expressed by those who chose to provide a further explanation for their response in the optional free text box (n=134). Many respondents who provided additional comments believed that a targeted ban on ransomware payments for CNI owners and operators and public sector would act as a deterrent and disincentivise attackers.

A small portion of respondents flagged the need for government support, including regulatory measures and incentives, guidance documents, financial investment and support for organisations in strengthening their cyber security.

[4] This category includes, CNI, local government, central government/civil service, and other public sector/public body.

Many respondents further identified the need for those covered by the targeted ban to improve and harden unsecure computer systems, and organisations' defence strategies and contingency plans, where vulnerabilities exist. This included wider supply chains regardless of where they sit in UK infrastructure.

A further portion of respondents reflected on the importance of enhanced recovery and incident response measures for organisations to improve their resilience:

> *"[It is] crucial to ensure robust incident response mechanisms and support for affected organisations to mitigate risks and maintain continuity of critical operations". –* ***Individual Respondent***

Several respondents also called for exceptions to a targeted ban, including consideration of the wider impact and where there would be severe consequences, such as in schools and hospitals.

> *"This ban must be accompanied by exemptions for extreme cases and increased government support for cybersecurity investments. Without these measures, affected organisations may struggle with recovery, and critical services could be at risk. A well-balanced approach, integrating prevention, preparedness, and strict compliance, is essential for the ban's effectiveness."* ***– Organisation Respondent***

However, some respondents commented that the ban should go further than CNI and the public sector, and include the private sector, supply chains, and key associates of CNI organisations. A few respondents also suggested that a clearly defined scope of the CNI sector would be necessary.

A few respondents were concerned about how this proposal will be managed across multiple jurisdictions, such as companies with headquarters outside of the UK, and the potential for making payments via non-UK entities. Respondents addressed the need to consider extraterritorial oversight and having clear legal boundaries.

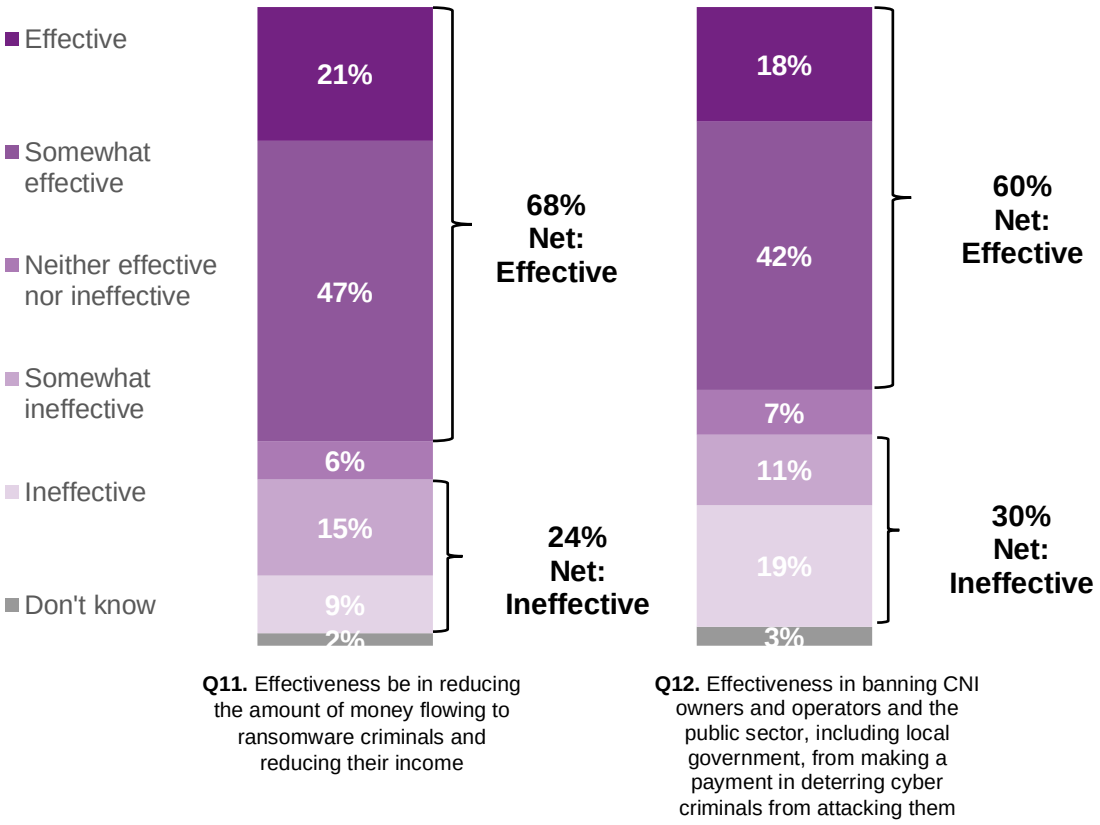
Additional prose responses that were supportive of this proposal believed it would act as a deterrent and reinforce cyber resilience. They also suggested that there needed to be a clear definition of CNI and essential services, especially in relation to financial and insurance sectors.

Questions 11 and 12

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

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

Figure 4: Perceived effectiveness of a targeted ban on ransomware payments for CNI owners and operators and the public sector for reducing the amount of money flowing to ransomware criminals (Q11) and deterring cyber criminals from attacking them (Q12)



Q11. *How effective do you think the proposed measure will be in reducing the amount of money flowing to ransomware criminals, and thus reducing their income?* ***Q12.*** *How effective do you think banning CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, from making a payment will be in deterring criminals from attacking them?* ***Base*** *= All respondents. Q11 (n=230) and Q12 (n=231)*

Overall, just over two thirds of respondents (68%) thought that a targeted ban will be effective in reducing the amount of money flowing to ransomware criminals, thus reducing their income.

A slightly higher proportion of individuals thought that this measure would be effective (70%), compared to organisations (65%) and a slightly higher proportion of CNI/public sector respondents thought this measure would be effective (74%), compared to those who did not respond as CNI/public sector (66%).

Six in ten (60%) respondents also thought that a targeted ban will be effective in deterring cyber criminals from attacking those organisations subject to the ban.

Over two thirds (68%) of those responding as individuals thought this measure would be effective, compared to just over half (54%) of those responding as an organisation. A

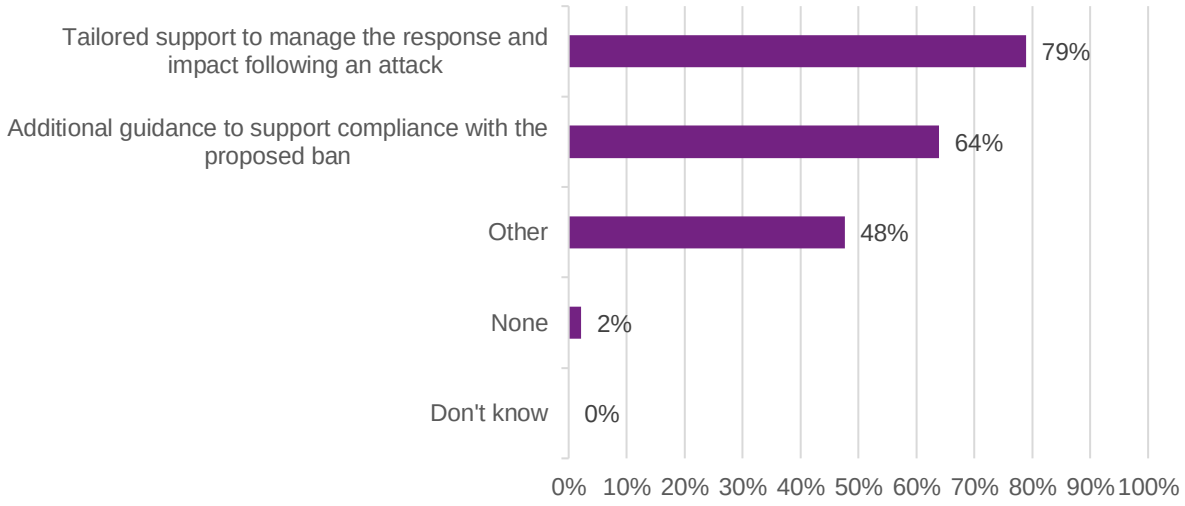
larger proportion of CNI/public sector respondents thought this measure will be effective at deterring cyber criminals (79%), compared to those who did not respond as CNI/public sector (54%).

Question 13

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

Respondents were able to select more than one option for this question. Over three quarters (79%) thought that tailored support to manage the response and impact following an attack would aid compliance with the proposed ban and nearly two thirds (64%) thought that additional guidance would support compliance. However, nearly half (48%) responded 'Other' to identify different measures. Only a small proportion (2%) thought no measures would aid compliance.

Figure 5: Views on measures for aiding compliance with a targeted ban



Q13. *What measures do you think would aid compliance with the proposed ban?* ***Base*** *= All respondents (n=233)*

A range of views were expressed by respondents selecting 'Other' (n=105).

Several respondents commented on the need for stronger guidance on implementing effective controls:

> *"Clear, accessible guidance is critical for organisations to understand their obligations under the proposed ban, including reporting requirements and compliance protocols."* ***– Organisation Respondent***

However, others thought that guidance alone was not sufficient and would need to be supported by other measures, such as strong regulations and audits for organisations:

> *"If this move is made [targeted ban] then there needs to [be] regulations that are strong and [auditable]…Simply having guidance is not sufficient*." ***– Organisation Respondent***

Some of the prose responses similarly commented on the need to have clear guidance on the implementation of the proposed ban, including enforcement, who is responsible for paying a ransom, and tailored advice.

Other suggestions included:

- Having public registers either showing organisations that are willing to comply with the ban or have chosen to pay a ransom
- Sharing a template for internal policies for preparing for and responding to a ransomware incident
- Promoting rewards or financial incentives for organisations that implement ransomware mitigation strategies e.g. grants or tax reductions

Many respondents identified various preventative measures, such as:

- Promoting defence strategies to better prepare organisations for an attack
- Investing in additional funding to enhance cyber resilience
- Requiring organisations to have a mandatory spend on security
- Providing security support and assistance prior to an attack to ensure robust backup and restoration processes

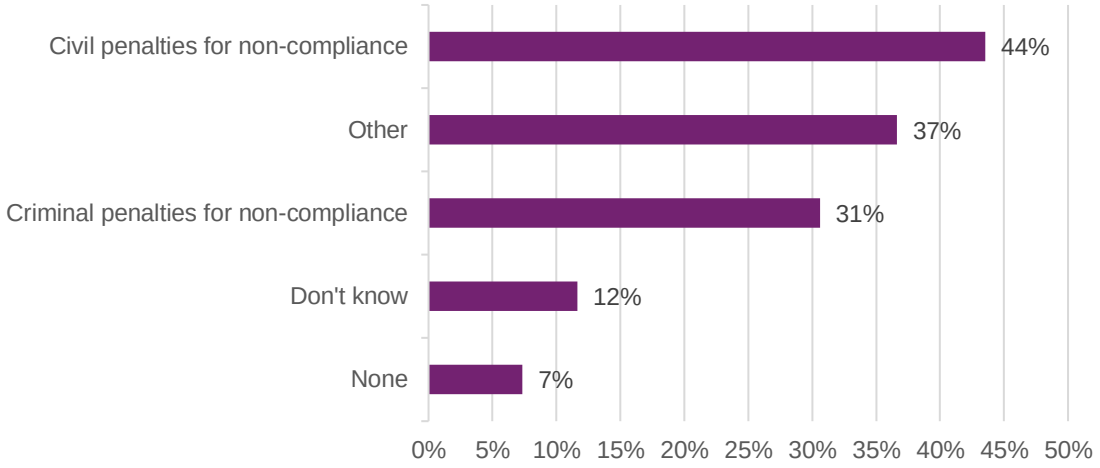
For those responding ‘None’, free text responses indicated that they did not believe this ban would be effective and was not an issue that needed legislation.

Question 14

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

Respondents could select multiple options for this question. Just under half (44%) thought civil penalties would be appropriate for non-compliance with the proposed ban and nearly a third (31%) thought that criminal penalties would be appropriate. However, over a third of respondents (37%) responded ‘Other’ and a small proportion (7%) thought no measures are appropriate for non-compliance.

Figure 6: Respondents' views on appropriate measures for non-compliance with a targeted ban



Q14. *What measures do you think are appropriate for non-compliance with the proposed ban?* ***Base*** *= All respondents (n=232)*

Those responding 'Other' provided suggestions across civil and criminal penalties (n=80). Civil penalties suggested included organisational level measures such as changes in leadership, repercussions and punishments for senior management, and public reporting on non-compliant agencies.

Suggestions for criminal penalties included sanctions, the extension of existing measures, and criminal measures specifically for leadership and management responsible for any decision making.

For both civil and criminal penalties, respondents identified the need to make penalties proportionate and at an appropriate level for those responsible:

> *"When addressing non-compliance with the proposed ban, it is essential to ensure that measures taken are appropriate and proportionate to the circumstances… the Competent Authority should have the discretion to consider all the circumstances and not be obligated to impose a penalty automatically."* ***– Organisation Respondent***

> *"Potentially criminal penalties are appropriate for persons directly responsible in the event of wilful and intentional non-compliance."* ***– Organisation Respondent***

Respondents also suggested this could potentially be on a case-by-case basis. For example, in relation to annual turnover, availability of the business service, and the impact on business function.

Respondents recognised concerns with the use of penalties, for example difficulties with enforcement, belief this will criminalise victims, and concerns that these measures may cause victims to not report.

Those who responded 'None' were able to provide further explanation (n=11). They provided similar reasons to those raising concerns around penalties, including this proposal not tackling the cause of the problem, potentially punishing or revictimising victims, and believing that penalties will be counterproductive:

> *"Penalising organisations for non-compliance is counterproductive and risks discouraging transparency and reporting. Criminal or civil penalties could push incidents underground, reducing visibility into ransomware threats and hindering collective efforts to combat them."* ***– Organisation Respondent***

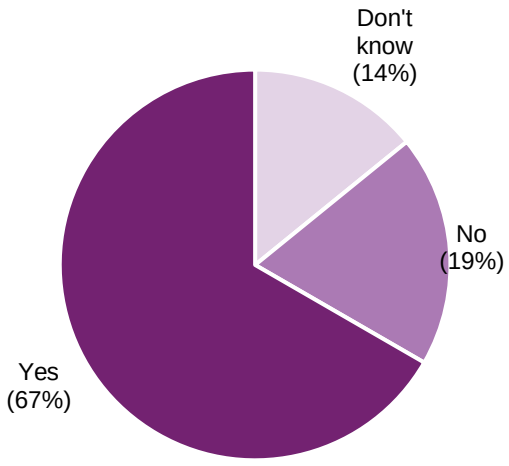
From the prose responses, respondents preferred the use of civil penalties over criminal penalties. However, there was concern that any type of penalty could revictimise and impose additional operational and financial burdens on victims.

Question 15

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

This question was directed at CNI/public sector organisations, but any respondent had the opportunity to respond, therefore it is possible that some respondents to this question do not represent the CNI/public sector. Of those answering this question, nearly two thirds (67%) said they would need additional guidance to support compliance with a ban on ransomware payments, and just under a fifth (19%) said that they would not.

Figure 7: Whether CNI/public sector organisations need additional guidance to support compliance with a ban on ransomware payments



Q15. *If you represent a CNI organisation or public sector body, would your organisation need additional guidance to support compliance with a ban on ransomware payments?* ***Base*** *= All respondents (n=99)*

Of those who responded that they would need additional guidance to support compliance and provided further information on this (n=55), a majority gave further details on the support that they would need. Their responses emphasised the need for improved guidance. For example:

> *"There will need to be clear, visible and accessible guidance… Whilst many may have these in place already, any guidance will need updating."* ***- Other Respondent***

Examples of areas this guidance should address included:

- What they should do if attacked
- Who and where to report incidents
- What options are available to them when they are attacked
- Contact information for support systems and incident response specialists
- How to facilitate effective communication between victims and attackers
- An outline of clear restrictions for making payments for example, if parent companies are headquartered abroad and the sectors included

A considerable portion of respondents identified the need for additional resources and funding support to address disruption costs, update IT systems, and support in the decision-making processes when an attack occurs.

> *"Most organisations require additional resources, including upgrading legacy IT systems."* ***– Organisation Respondent***

Respondents also wanted access to more training and awareness sessions on what to do if there was an attack, and to educate organisations on capacity building and cyber resilience, including tailored consultation and expert advice.

> *"There should be awareness sessions organised explaining what the process is and why it is done that way."* ***– Individual Respondent***

> *"Provision of up-to-date knowledge, standard guidelines/enforcement procedures. Helplines/reporting lines. Training on what steps to undertake if subject to ransomware attack."* ***– Organisation Respondent***

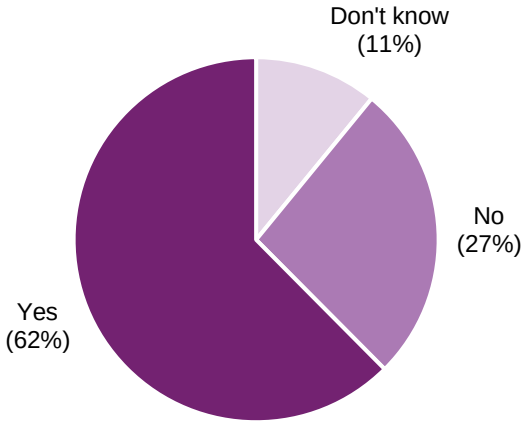
They also identified the need for seniors and management to have a good understanding of ransomware guidelines, and to have top-down accountability in sharing this information.

Question 16

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

Around six in ten respondents (62%) said that organisations within CNI and public sector supply chains should be included in the proposed ban, and just over a quarter (27%) said that they should not be included.

Figure 8: Whether organisations within CNI and public sector supply chains should be included in the proposed targeted ban



Q16. *Should organisations within CNI and public sector supply chains be included in the proposed ban?* ***Base*** *= All respondents (n=229)*

Respondents who selected 'Yes' or 'No' could give additional explanation (n=156). Reasons given why the proposed measures should apply to organisations in CNI and public sector supply chains included:

- Their critical role in the wider ecosystem
- That they are often targets for ransomware attacks
- Supply chains are interconnected, so a ransomware attack can impact a lot of sectors and cause widespread damage

Some also believed that these measures should be extended to all companies, including private companies, as an attack anywhere could potentially have a significant negative impact.

However, some respondents flagged several issues with including CNI and public sector supply chains in the proposed ban. These included:

- Difficulty in defining the scope due to complexity of supply chains
- Existing restrictions on supply chains and areas of CNI/public sector
- Supply chains being too weak to handle additional restrictions
- Additional measures could disproportionately impact smaller businesses, or potentially revictimise organisations that have been attacked

Some felt that particular areas of CNI are too critical to be included in these measures and there should be case-by-case consideration based on impact and the role of each organisation within the supply chain.

> *"CNI provides essential services whose disruption could have severe consequences for society. Therefore, swift recovery of these services is paramount, sometimes making ransom payment a necessary compromise."* ***– Other Respondent***

Several respondents identified the necessity of providing supply chains with support to ensure they can adapt and strengthen their resilience:

> *"Efforts should focus on incentivising preventive measures, strengthening resilience, and providing tailored support for recovery to minimise reliance on ransom payments".* ***– Organisation Respondent***

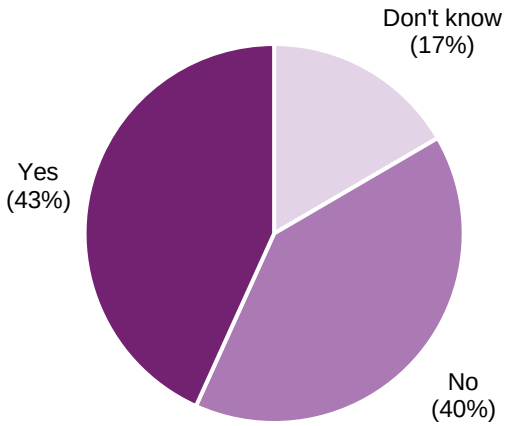
There were mixed views from prose responses about expanding the ban to include CNI and public sector supply chains. Some believed including them could significantly broaden the scope of the proposal to become an economy-wide ban and will have a disproportionate impact on the UK's ability to effectively respond to the ransomware threat. Other respondents commented that not including them will make them targets.

Question 17

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

Views were almost evenly split in terms of whether there should be exceptions to the proposed ban, with around four in ten thinking there should be (43%) and a similar proportion (40%) thinking that that there should not be exceptions.

Figure 9: Whether there should be any exceptions to the proposed ban



Q17. *Do you think there should be any exceptions to the proposed ban?* ***Base*** *= All respondents (n=229)*

Respondents in support of exceptions could provide further explanation (n=84). The main reason given focused on concerns about the impact of non-payment on critical services, national security or if there was a threat to life.

> *"Exceptions could be considered in cases where national security or public safety is at immediate risk, and making a payment is the only viable option to prevent catastrophic consequences. Such exceptions should be tightly regulated and require high-level approval."* ***– Individual Respondent***

Several respondents also identified the need for consideration to be on a case-by-case basis to understand the context of the attack.

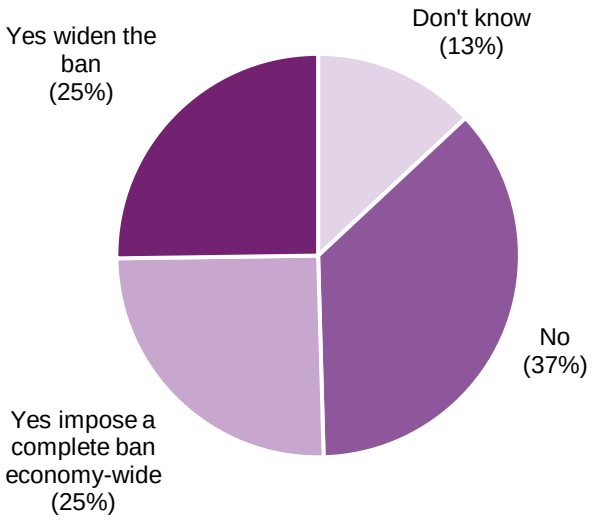
Prose responses emphasised the need to consider including exemptions in exceptional circumstances when all other recovery options have been exhausted, especially if payment can restore critical functions or prevent widespread harm.

Question 18

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

In total, half of respondents (50%) thought that the ban should be expanded in some way, this was a quarter of all respondents thinking it should be widened (25%) and another quarter thinking it should be economy-wide (25%). However, over a third of all respondents (37%) thought that there was not a case for widening the ban or for imposing a complete ban economy-wide.

Figure 10: Whether there is a case for further widening the ban on ransomware payments or imposing a complete economy-wide ban



Q18. *Do you think there is a case for widening the ban on ransomware payments further, or even imposing a complete ban economy-wide (all organisations and individuals)?* ***Base*** *= All respondents (n=230)*

Those in favour of widening the ban could provide further explanation for their response (n=45). A considerable portion of respondents identified suggestions for widening, for example, the inclusion of other sectors, basing inclusion on turnover, and starting with CNI then expanding to small businesses.

There was a wide variety of explanations for this response, including believing widening the ban would stop money flowing to criminals, prevent any loopholes that could be exploited, reducing the attractiveness of UK targets and reduced incentives for attackers.

However, several respondents still flagged concerns here with widening the ban. For example, around uncertainty of including individuals in the ban, concerns on the proportionality and consistency across all those included in the ban, and a lack of consideration for organisations' existing quality of IT and resilience.

Government policy response

Overall, the consultation responses demonstrated strong support for a targeted ban on ransomware payments. The Government will continue to develop this proposal in collaboration with industry.

Feedback received indicated broad support for the overall aim of the proposal. However, it clearly articulated a need for further clarity on the scope and definition of who would be included in such a ban, including whether the proposal would have extraterritorial effect. The Government intends for any potential measures and associated guidance to clearly explain the scope of the ban.

There was mixed feedback on what the penalties should be for non-compliance with this proposal, including concerns about revictimising victims. The Government will continue to explore the most appropriate and proportionate penalties.

Respondents clearly indicated that extra support would be required for compliance, including additional, sector-tailored guidance and resilience measures. The Government will consider this across the policy response to ransomware and cyber security more broadly and will publish additional guidance alongside any legislation.

There was positive feedback that supply chains should be part of the ban. However, complexities of implementation were flagged, including that suppliers could need additional support to ensure compliance. The Government will explore existing arrangements under the Cyber Security and Resilience Bill and other measures such as the reporting work being undertaken by the Bank of England, and existing sectoral reporting requirements. The Home Office is working with lead critical national infrastructure government departments to consider the most appropriate approach for supply chains.

There were also mixed responses on whether the proposed ban should include a mechanism for exceptions, with those in favour of exceptions citing national security or public safety as key reasons.

Half of respondents (50%) thought that the proposed ban should be expanded, with a quarter of all responses thinking it should be widened (25%) and another quarter thinking it should be economy-wide (25%). However, over a third of all respondents (37%) thought

that there was not a case for widening the ban, or for imposing a complete ban economy-wide. The Government will consider this feedback.

Feedback received through the events and ongoing industry engagement included questions around liability for compliance with the proposals. This was particularly raised with reference to financial institutions who could be asked to process potentially illegal payments on behalf of victim organisations (either under the targeted ban or ransomware payment prevention regime). The Government is exploring liability holistically across the proposals, as well as directly with the finance sector through continued technical discussions.

Proposal 2

Proposal summary

A new ransomware payment prevention regime to cover all potential ransomware payments from the UK.

The regime would require ransomware victims to report their intent to pay to the Government via a central mechanism. After the report is made, the victim would receive support and guidance. The Government would then review the proposed payment. A payment may be blocked where it could go to criminals subject to sanctions designations, or in violation of terrorism finance legislation. If the proposed payment is not blocked, it would be a matter for the victim whether to proceed. Payments would not be approved under this regime. The Government does not advise paying ransoms.

Analysis summary

Question 19

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

There were mixed agreement levels across the suggested measures for Proposal 2, but overall analysis of both the survey and free text responses suggests a slightly stronger preference for economy-wide over threshold-based measures. This analysis is discussed in more detail below.

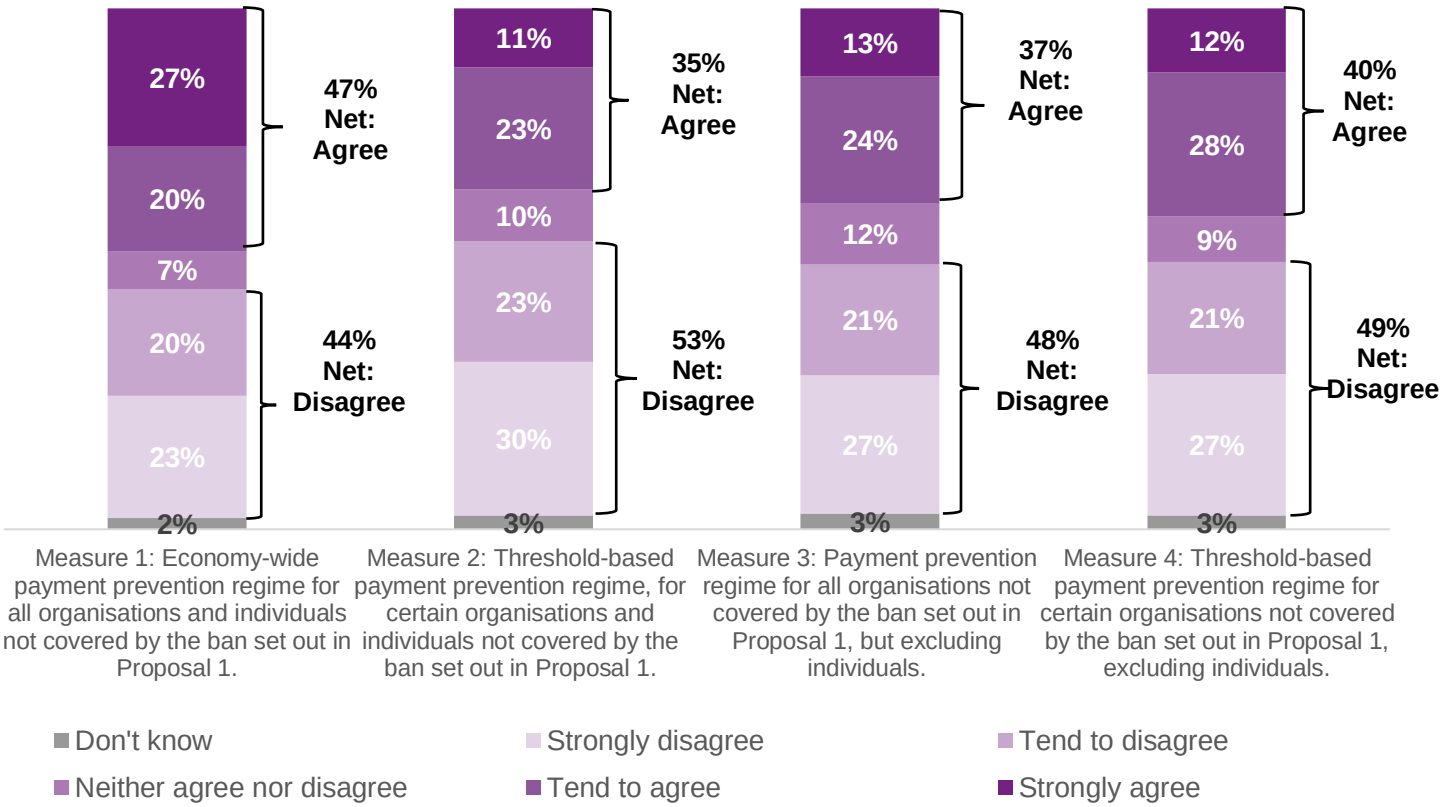
Views overall were fairly evenly split on whether the Home Office should implement *'Measure 1: Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1'*, with nearly half of respondents agreeing (47% net agreement) and a similar proportion disagreeing (44% net disagreement). However, this was the highest level of agreement across all four measures and notably 'Measure 1' had the highest proportion of respondents who 'strongly agreed' to implement (27%, compared to 11-13% for other measures). Moreover, larger proportions of respondents overall disagreed with implementing Measures 2 - 4 than who agreed (48 – 53% levels of net disagreement).

When considering respondents characteristics, it should be noted that agreement with Measure 1 is driven primarily by individuals, as nearly two thirds of individuals (64%) agreed with this measure, compared to just over a third of organisations (36%).

Levels of disagreement varied slightly across individuals and organisations for Measures 2-4:

- *'Measure 2: Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1'* - levels of disagreement were similar across individuals (52%) and organisations (54%)
- *'Measure 3: Payment prevention regime for organisations not covered by the ban set out in Proposal 1'* - a slightly lower proportion of individuals disagreed with this measure (45%) compared to organisations (50%)
- *'Measure 4: a threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1'* - a slightly higher proportion of individuals disagreed with its implementation (54%), than the proportion of organisations who disagreed (46%)

Figure 11: Agreement levels for implementing different legislative measures for a new ransomware payment prevention regime



Q19: *To what extent do you agree, or disagree, that the Home Office should implement the following legislative measures.* ***Base*** *= All (n = 230 for Measures 1, 2, and 3; n=228 for Measure 4)*

A range of views were expressed by those choosing to provide further explanation for their response (n=102). A considerable portion identified issues with a threshold-based payment ban, including the potential for loopholes, the risk of criminals changing their methods and/or targets to attack organisations not covered, and a general view that this measure would be ineffective.

> *"We have concerns that the action of setting thresholds for payment may lead to cyber criminals tailoring their ransomware demands to suit, targeting those organisations below any threshold and potentially seeking to operate at higher volumes (i.e. more and more frequent attacks) in order to improve revenue."* - ***Organisation Respondent***

A few respondents disagreed with the inclusion of individuals in a payment prevention regime; reasons included them not having access to the same resources or understanding of cyber security as large organisations. However, some of these respondents identified that not including individuals could create a loophole for attackers to target business officials or key persons within an organisation as individuals rather than the business.

Some respondents also identified ways that the above measures could tailor the threshold. For example, considering the organisation's geographic location, area of operation and size and the risk level of paying, or not paying a ransom. A few respondents also suggested starting with the CNI/critical supply chains before expanding further.

Additional prose responses were concerned about the resource and capacity required to implement a payment prevention regime on an economy-wide scale. This was also due to the time sensitivity associated with making decisions on ransomware payments.

Prose respondents also wanted further clarity on details of the ransomware payment prevention regime, including the role of third-party payment facilitators, key legislation to support enforcement of this proposal, financial support, and clarity on the decision-making process.

A small majority of respondents provided more general suggestions on additional support, including education on appropriate security measures, recovery plans, and victim support such as incident response resources.

Questions 20 and 21

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

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

Respondents were asked how effective they think the suggested measures will be in reducing ransomware payments and, separately, in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors. There were mixed effective responses across all measures.

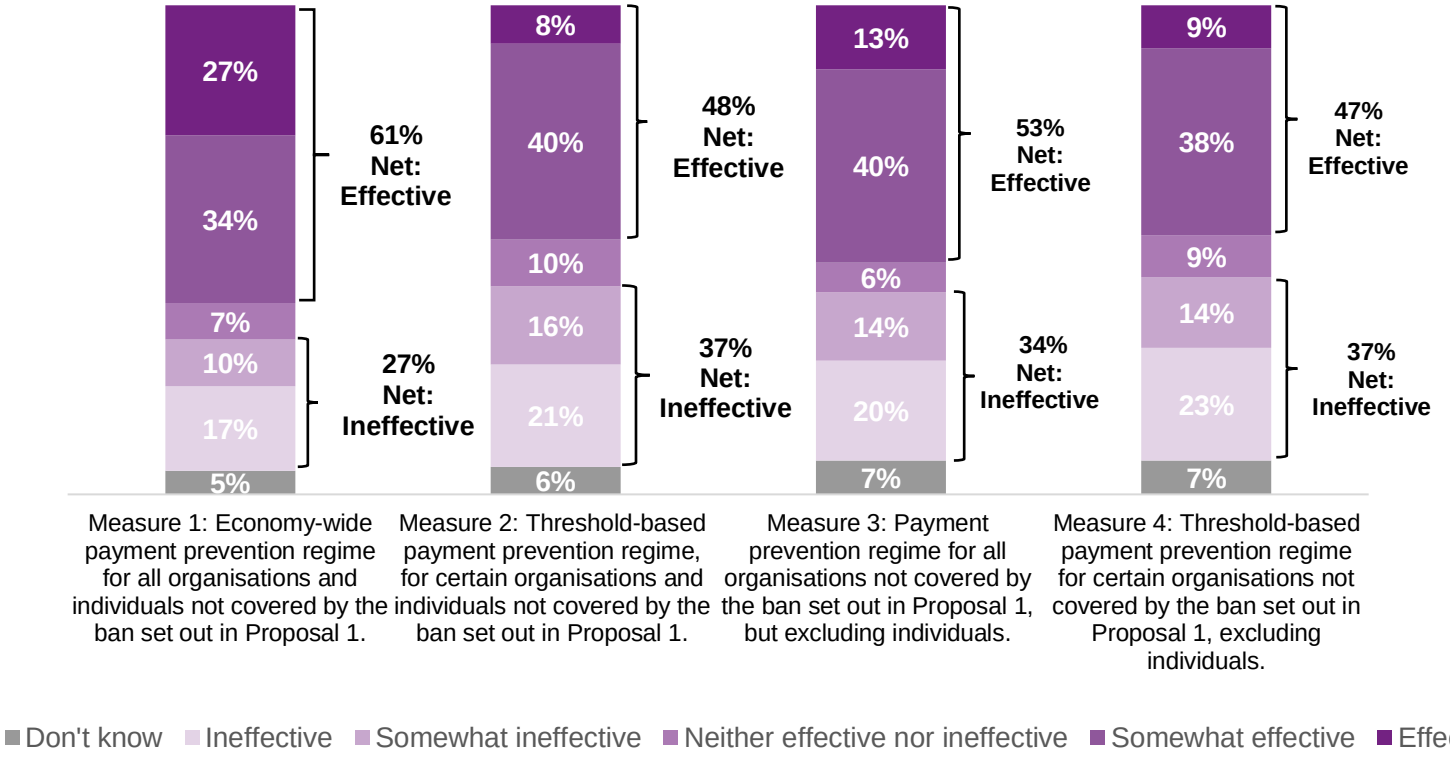
'Measure 1: an economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1' had the highest proportion of respondents who thought it would be 'effective' in reducing ransomware payments (27% compared to 8-13% for other measures) and in increasing the ability of law enforcement agencies to intervene and investigate (22% compared to 9-11%).

A higher proportion of individuals thought Measure 1 would be effective in reducing ransomware payments (71% net effective), compared to just over half of organisations (54% net effective).

Across all measures, a larger proportion of respondents selected that they thought the measure would be effective at reducing payments, compared to the proportion that thought the measure would be effective at increasing law enforcement's ability to intervene and investigate actors.

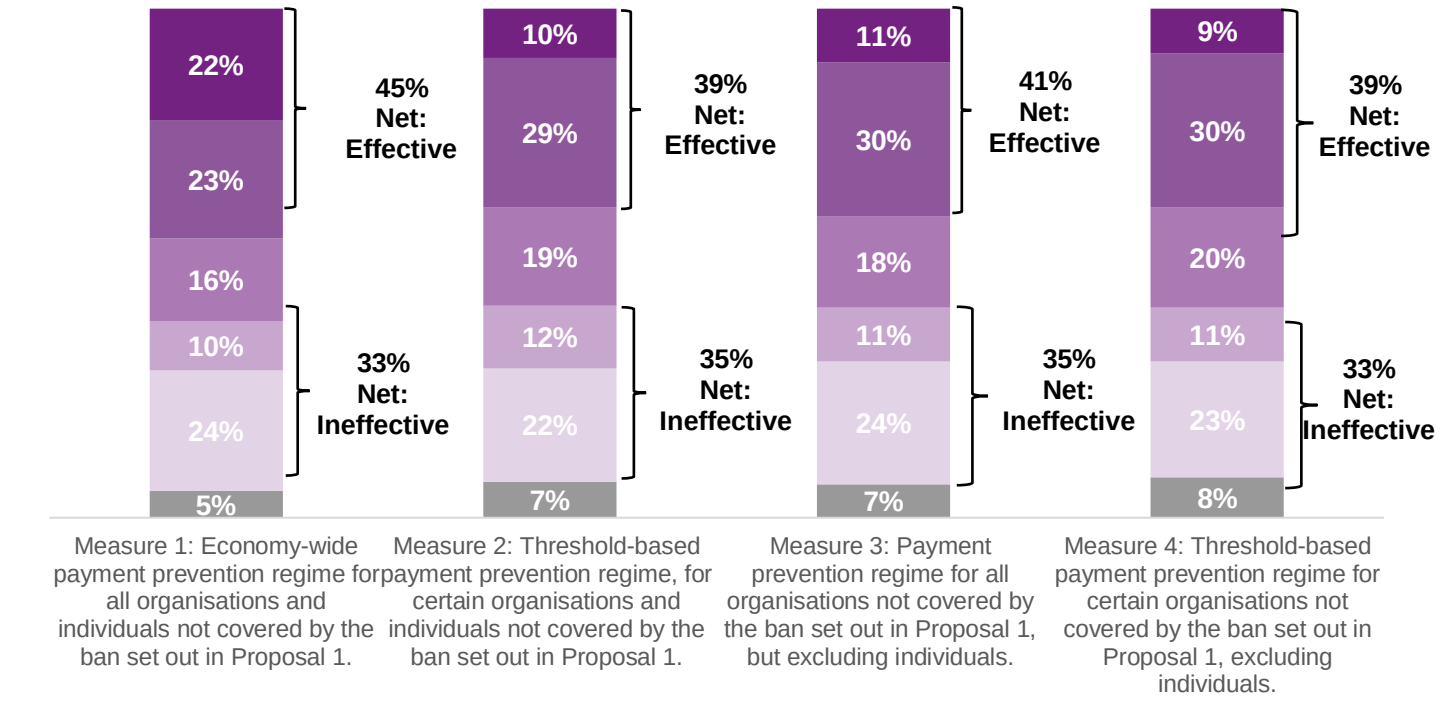
More respondents (around 20%) also thought that these measures would be neither effective, nor ineffective, in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors, than when asked about how effective these proposals would be for reducing ransomware payments (around 10%). This suggests perhaps more uncertainty, or lower confidence, in respondent ability to comment on this type of potential impact.

Figure 12: Perceived effectiveness of a new ransomware payment prevention regime in reducing ransomware payments



Q20: *How effective do you think the following will be in reducing ransomware payments?* ***Base*** *= All (n=230)*

Figure 13: Perceived effectiveness of a new ransomware payment prevention regime in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors



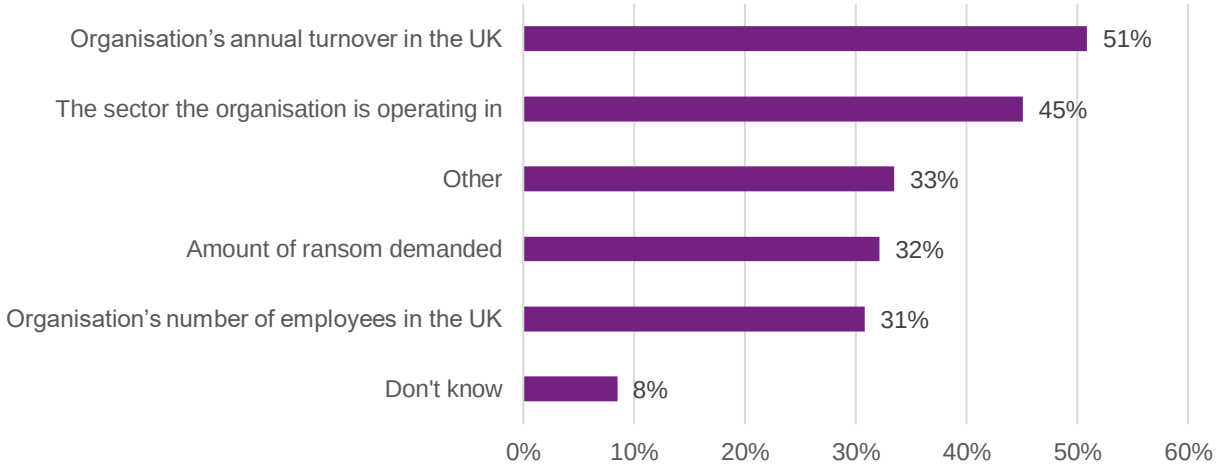
Q21: *How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors?* ***Base*** *= All (n=228)*

Question 22

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

For this question respondents could select multiple options. They thought there were several key approaches to best determine the threshold for inclusion for a threshold-based payment prevention programme. Just over half (51%) thought annual turnover in the UK would be appropriate and just under half selected by sector (45%). Around a third of respondents thought that the amount of ransom demanded (32%) and organisation's number of employees in the UK (31%) would be good ways to determine the threshold for inclusion.

Figure 14: Perceptions on best determining the threshold



Q22: *If we introduced a threshold-based payment prevention regime, what would be the best way to determine the threshold for inclusion?* ***Base*** *= All (n=224)*

A third of respondents selected 'Other' (33%) and were given the opportunity to provide explanations (n=75). Many of these respondents identified ways of tailoring the threshold for inclusion, suggestions included:

- The nature of the organisation attacked. For example, an attack on a critical financial technology firm could threaten financial stability
- The impact of the attack on victims or wider society, including the ability for organisations to operate their services, impact of exposing or losing data, or geopolitical risks
- Taking a proportionate approach in relation to the size of organisation
- Their level of compliance with measures and with cyber security legislation

Many respondents still expressed that a threshold-based payment prevention regime would be ineffective and not a suitable measure. There was concern that a threshold-based payment regime would push ransomware attackers to change their tactics and targets to target organisations below any threshold, seeking to operate at higher volumes and damaging smaller businesses.

> *"All methods listed above would simply result in the target of ransomware attacks shifting. Imposing a threshold would be especially damaging as businesses with lower numbers of employees or turnover who would be more likely to be targeted as a result will also not have the same resources behind them to deal with any incidents."* ***– Individual Respondent***

Additional prose responses commented on including a threshold for a payment prevention regime. Some respondents suggested options for creating a threshold, including organisation size, annual turnover, sector type, or number of employees. However, other

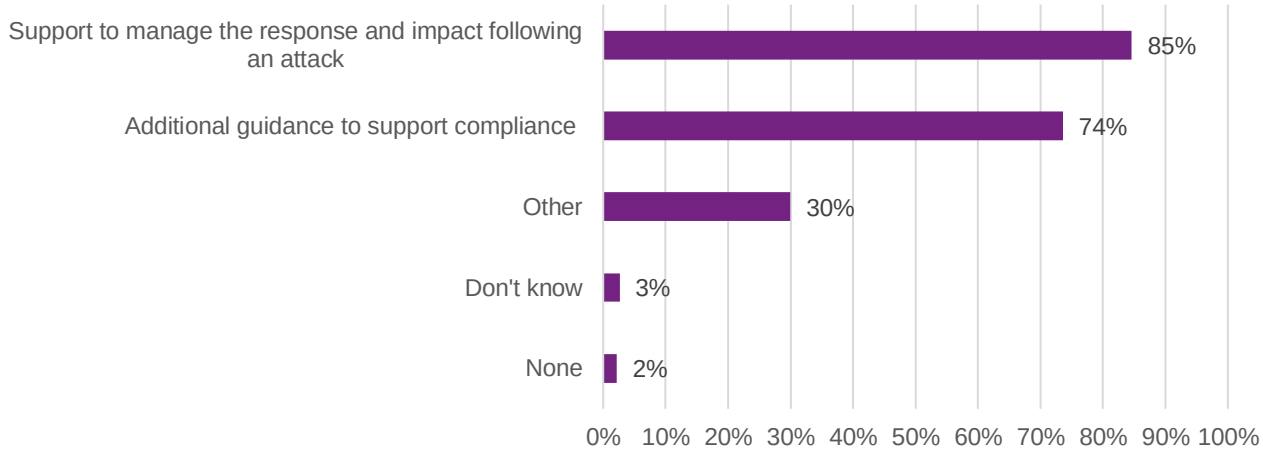
respondents suggested all payments should be reported and that thresholds can create victim targets.

Question 23

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

For this question, respondents could select multiple options. They thought that support to manage the response and impact following an attack (85%) and additional guidance to support compliance (74%) would help aid compliance with a payment prevention regime. Only 2% thought that there would be no measures that would aid compliance.

Figure 15: Respondents' views on measures to aid compliance with a payment prevention regime



Q23: *What measures do you think would aid compliance with a payment prevention regime?* ***Base*** *= All (n= 227)*

Just under a third of respondents (30%) thought that there were 'Other' measures that would aid compliance. Respondents who selected 'Other' could provide further details (n=64).

Many respondents expanded on the need for additional guidance and support by focusing this on prevention. This included:

- Strengthening operational resilience
- Guidance on important legal obligations
- Education and publicity campaigns to spread awareness
- Sector specific guidance

It was suggested that these should be supported by communication from the Government on details of the legislation, and why and how the measure is effective:

> *"One measure which could aid compliance is clear and consistent communication from government… government should be clear about why reporting requirements are being introduced and how the information provided by industry will be used."* **– *Organisation Respondent***

A small majority of these respondents suggested post-incident support as an important measure to aid compliance. Examples included providing robust prevention and recovery solutions, technical audits of control, sector specific unit response, and engagement with the insurance industry.

> *"The Government must take a balanced approach that combines clear guidance and robust support mechanisms with meaningful incentives for organisations."* **– *Organisation Respondent***

Other measures respondents suggested to aid compliance included financial incentives, mandatory reporting and provision of additional funding.

> *"Sector-specific response unit, real-time intelligence sharing, and cybersecurity funding support."* **– *Organisation Respondent***

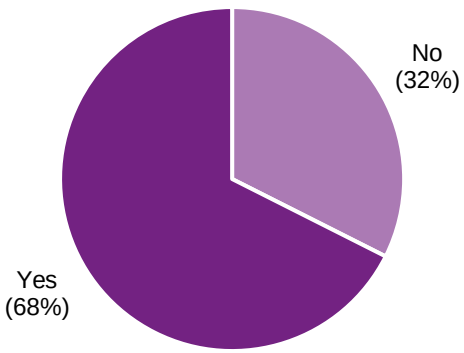
For those responding 'None', responses indicated similar views around focusing on improving cyber awareness and resilience. There were also concerns about using penalties for non-compliance and how the regime could impact on the economy. Limited further information was given on this.

Question 24

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

Over two thirds of respondents (68%) thought that any compliance measures would need to be tailored to different organisations and individuals.

Figure 16: Whether compliance measures need to be tailored to different organisations and individuals



Q24: *Do you think these compliance measures need to be tailored to different organisations and individuals?* ***Base*** *= All (n=222)*

Respondents who thought that compliance measures need to be tailored could give further details (n=105). They provided a range of suggestions for how to tailor compliance measures, including:

- Size of organisation
- Organisation type e.g. public sector, charity, private sector
- Complexity of IT systems
- A tiered approach based on risk profile/critical nature of targeted organisation
- Amount of resources available to organisation
- Sector specific guidance

A notable portion of respondents specifically suggested that it was response and recovery options that should be tailored.

> *"Response and recovery operations need to be tailored as different organisations have different priorities for which parts of IT infrastructure are operable, and have vastly different scale and technology selection. Different recovery assistance plans should exist for broad categories of priority and scale."* ***– Individual Respondent***

Several respondents provided more details on the need for support and guidance to aid compliance. This included:

- Support in returning to an operational state after an attack
- Support and guidance in identifying risks
- Enhanced support for CNI sectors
- Support for management levels

A few respondents also suggested that larger organisations can handle stricter requirements, such as audits or reporting standards, as they have larger budgets and resources and should be held to a higher standard than smaller organisations.

> *"Small businesses may need simplified guidance and low-cost solutions, while larger organisations require detailed frameworks and advanced tools."* ***– Individual Respondent***

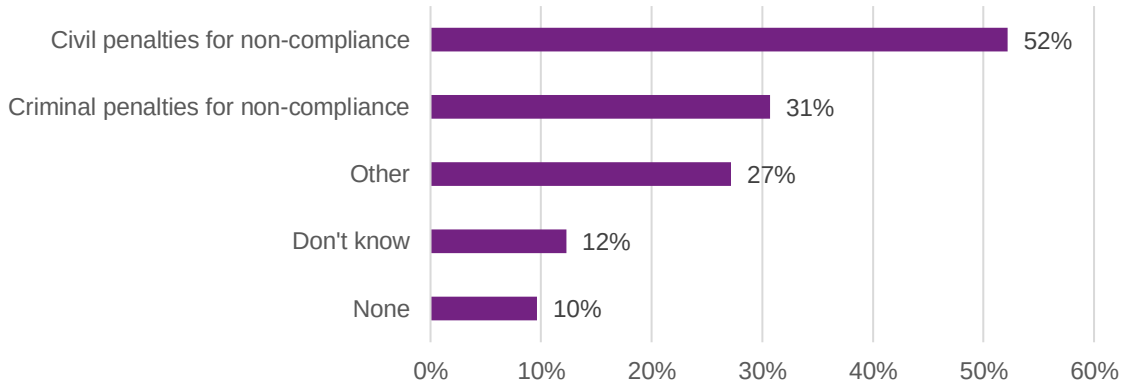
Prose respondents also identified that compliance measures should be tailored, especially where there may be differences in the complexity of demands, size of the ransom and types of sectors affected.

Question 25

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

Respondents selected all responses that applied to them. Just over half (52%) thought that civil penalties would be appropriate for non-compliance with a payment prevention regime and under a third (31%) thought that criminal penalties would be appropriate.

Figure 17: Respondents' views on appropriate measures for managing non-compliance with a payment prevention regime



Q25: *What measures do you think as appropriate for managing non-compliance with a payment prevention regime?*
Base *= All (n=228)*

Just over a quarter of respondents (27%) responded 'Other' and could provide further information (n=58).

A small majority provided further details on the types of penalties that could be used. For civil penalties: publicly naming organisations that fail to comply; financial penalties and pairing civil penalties, with additional monitoring and auditing to ensure future compliance. For criminal penalties, these were deemed appropriate in extreme cases of intentional non-compliance or specifically for senior management.

Several of these respondents noted that any measures to manage non-compliance should be proportionate and tailored, with a graduated enforcement. This included considering, size of the organisation, the extent, severity and complexity of the attack, and amount of the ransom.

> *"Penalties should be balanced and proportionate to the effects of ransomware and should avoid penalising victims."* ***– Organisation Respondent***

Several respondents suggested the provision of supporting and encouraging organisations rather than promoting penalties. This included safeguards to prevent data loss, promoting education and cyber awareness, and providing access to incident response and insurance support.

> *"Encouraging organisations to report incidents without the fear of punishment is essential for a collaborative approach to cybersecurity."* ***– Organisation Respondent***

Several respondents identified issues with civil and criminal penalties for non-compliance, including penalising victims who have already lost money, risks of causing underreporting, and believing any penalties to be unrealistic.

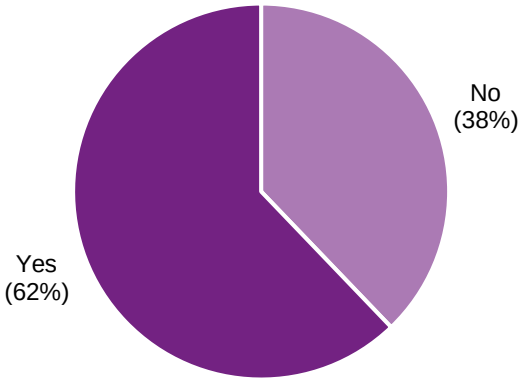
Respondents who thought there would be no appropriate measures (n=12) expressed similar views. They did not want penalties to criminalise or further punish victims and suggested offering educational support and financial incentives to victims.

Question 26

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

Most respondents thought that any non-compliance measures would need to be tailored to different organisations and individuals (62%).

Figure 18: Whether non-compliance measures need to be tailored to different organisations and individuals



Q26: *Do you think these non-compliance measures need to be tailored to different organisations and individuals?* ***Base*** *= All (n=222)*

Respondents who thought non-compliance measures need to be tailored to different organisations and individuals could provide further explanation (n=83). Many respondents reiterated the need for tailoring of the non-compliance measures, particularly that suitable deterrents will differ between organisations and individuals, and for organisations of different sizes, resources, and turnover.

Some respondents believed that non-compliance measures should not apply to individuals.

> *"For individuals, penalties should be avoided entirely, as they may lack the resources or expertise to comply fully."* ***– Organisation Respondent***

Respondents also suggested that measures of non-compliance could be tailored, depending on how compliant the organisation is, the type of victim for example, critical sectors or organisations, or the type of extorted data.

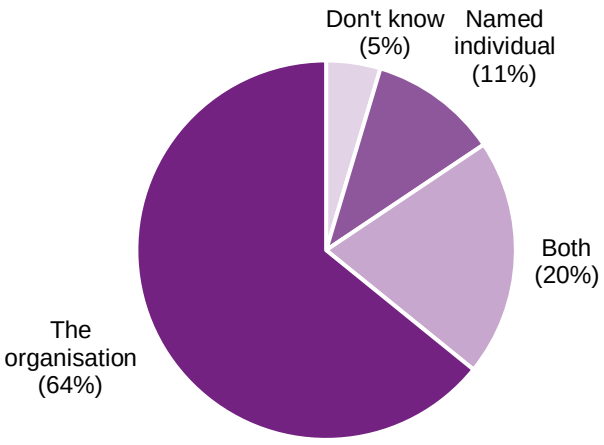
Prose respondents identified that non-compliance measures may need additional skills and resources for law enforcement agencies to investigate any breaches. For example, staff with technical skills (i.e. in cryptocurrency).

Question 27

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

Nearly two thirds of respondents (64%) thought that the organisation should be legally responsible for compliance with the payment prevention regime, and only just over one in ten (11%) thought that a named individual should be. A fifth of respondents (20%) thought that both the organisation and a named individual should be legally responsible.

Figure 19: Who should be legally responsible for complying with the regime



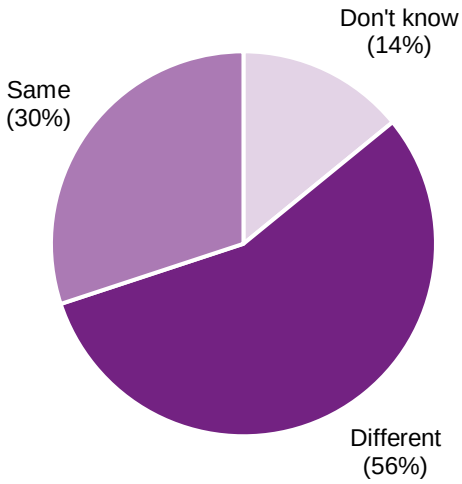
Q27: *For those reporting on behalf of an organisation, who do you think should be legally responsible for compliance with the regime?* ***Base*** *= All (n= 173)*

Question 28

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

Just over half of respondents (56%) thought that any measures for managing non-compliance with regime should be different for the organisation and a named individual responsible for a ransomware payment. Nearly a third of respondents (30%) thought that any measures for managing non-compliance should be the same for both.

Figure 20: Whether non-compliance measures should be the same or different for both the organisation and a named individual responsible for ransomware payments



Q28: *For those reporting on behalf of an organisation, do you think any measures for managing non-compliance with the regime should be the same for both the organisation and a named individual responsible for a ransomware payment?* ***Base*** *= All (163)*

Respondents could provide further explanation (n=55). There were mixed views on who should be responsible for ransomware payment. Several believed that a named individual should be responsible, as this would drive personal responsibility and liability from senior management to invest resources into cyber security and hold them accountable.

> *"If you put a named individual in the frame, their personal liability will mean they'll drive the action. If you make it an organisation problem, there isn't really an owner."* ***– Organisation Respondent***

However, respondents also identified that organisations ultimately make a collective decision to pay, so organisational-level measures are sufficient.

Most respondents identified a difference in responsibility between a named individual and organisation and believed non-compliance measures should reflect this. For example, an organisation may overrule a named individual, especially in the stress of a ransomware incident, so they may not be fully accountable for decisions made. Organisations could face larger penalties due to their scale and resources, while individuals could be held accountable based on their decision-making role.

> *"Organisations have the resources, authority, and systems to ensure compliance, and they should bear the primary responsibility. Named individuals often act under duress during ransomware incidents and may not have the autonomy to implement or enforce compliance measures."* ***– Organisation Respondent***

Government policy response

Feedback on the ransomware payment prevention regime has been mixed, when looking at the qualitative and quantitative responses together. The highest proportion of

agreement was for ‘Measure 1’ (an economy-wide regime for all those who are not included in the ban) to be introduced (47% net agreement). Fewer respondents supported Measures 2 - 4, which included threshold-based approaches and the exclusion of individuals. The Government will continue to develop this proposal.

There were mixed responses, across all measures, in how effective these measures would be in reducing ransomware payments and in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors. However, ‘Measure 1’ (an economy-wide regime) had the highest proportion of perceived effectiveness for both goals (61% and 45% responded it would be net effective respectively).

Respondents flagged various potential support measures and/or guidance that could be introduced. The Government will explore what could be introduced alongside this measure with the operational and policy community, ensuring alignment and complementarity with the Cyber Security and Resilience Bill.

It was felt that there should be different non-compliance measures for organisations and individuals. Within organisations, nearly two-thirds (64%) thought that the organisation should be legally responsible for compliance with the payment prevention regime. Only 11% thought that a named individual should be. A fifth of respondents (20%) thought that both the organisation and a named individual should be legally responsible. Over two thirds (68%) felt that there should be tailored compliance guidance for organisations and individuals. The Government will continue to explore the most proportionate approach by working with businesses, organisations, and law enforcement to provide robust, clear, and appropriate compliance guidance alongside the introduction of this measure. The Government will also consider any associated resource implications.

There was mixed feedback on what the penalties for non-compliance with this proposal should be, including concern that penalties could criminalise or revictimise victims. The Government will continue to explore what the most appropriate and proportionate penalties should be.

Beyond the consultation responses, and in wider engagement, the Government has continued to develop this policy. The Government’s intention is that all victims who have complied with the ransomware payment prevention regime would get proof of engagement to demonstrate to any payment broker or facilitator that they had adhered to the regime.

As discussed with reference to proposal one, the Government will continue to consider liability holistically with regards to the ransomware payment prevention regime and continue to engage with the finance sector in technical discussions.

Proposal 3

Proposal summary

A ransomware incident reporting regime that could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

A mandatory reporting requirement would mean that any victims of ransomware would be obliged to provide the Government with an initial report within 72 hours of the attack, covering key details, and a more in-depth report within 28 days.

The mandatory reporting requirement is intended to aid the Government and law enforcement's understanding of the scale, type and source of ransomware threats and assist with building intelligence and understanding. This will allow the Government, law enforcement, and organisations to build resilience, tailor responses, and engage in targeted disruptions in an evolving threat landscape.

The reporting requirements are not intended to be unnecessarily burdensome, and further work will be done to align any additional reporting requirements with existing pathways, as far as it is possible to do so.

Analysis summary

Question 29

Q29: To what extent do you agree, or disagree, that the Home Office should implement the following measures for a ransomware incident reporting regime?

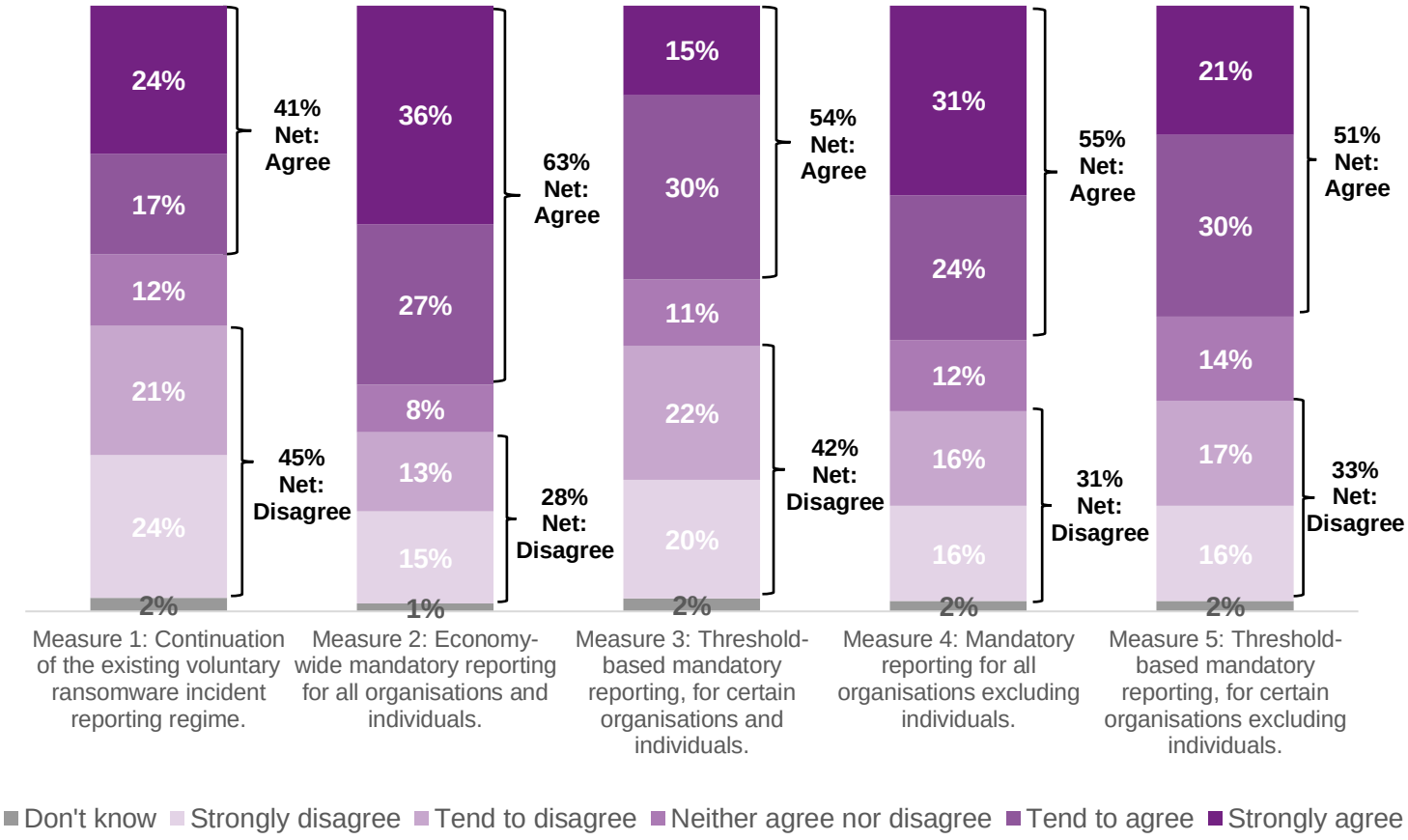
Responses show agreement that a new mandatory reporting regime should be introduced, as Measures 2-5 were viewed more favourably than Measure 1, proposing a continuation of the existing voluntary ransomware incident reporting regime.

'Measure 2: Economy-wide mandatory reporting for all organisations and individuals' had the highest proportion of agreement to implement, with nearly two thirds (63% net agreement) agreeing and around a third of respondents (36%) strongly agreeing. There were differences between individuals and organisations, with nearly three quarters (73% net agreement) of individuals agreeing compared to just over half (55% net agreement) of organisations.

Around half of respondents agreed with the other three new suggested measures (see Figure 21) and levels of agreement were relatively consistent across individuals and organisations.

Less than half (41%) of respondents agreed that the Home Office should continue the existing voluntary ransomware incident reporting regime.

Figure 21: Agreement levels for implementing different legislative measures for a ransomware incident reporting regime



Q29: *To what extent do you agree, or disagree that the Home Office should implement the following measures for a ransomware incident reporting regime.* ***Base*** *= All (Measure 1 n=229; Measures 2,3,4,5 n=230)*

Respondents were able to provide additional explanation for their responses (n=90). Most respondents provided additional responses in support of a mandatory reporting regime. Responses included:

- Believing that reporting will increase intelligence to better understand the threat landscape
- Suggesting aligning the regime with existing models and coordinating with industry partners and the Information Commissioner's Office (ICO)
- Believing mandatory reporting would avoid loopholes and ensure effective implementation

Several respondents thought that individuals should be excluded from a mandatory reporting regime and that it would be unrealistic for individuals to comply with. Some respondents suggested that individuals should be excluded unless sensitive information has been breached.

Several respondents suggested the use of a tiered approach to a reporting regime. This included adjusting reporting expectations for individuals, smaller organisations and larger organisations based on cyber security resources or severity of the incident.

> *"We recommend a tiered approach that allows for baseline reporting initially, with more comprehensive details following as the incident picture clarifies."* ***– Organisation Respondent***

> *"Considering a tiered reporting approach, scaled to organisational size, capacity, and sectoral risk."* ***– Organisation Respondent***

A few respondents also highlighted some potential issues or considerations for a mandatory reporting regime, including:

- Offenders demanding ransoms just below the threshold
- If individuals are excluded there may be a risk of organisations using this as a loophole
- Privacy and confidentiality concerns

Prose responses further expressed general agreement with the mandatory reporting regime, as it would assist with information sharing and building the ransomware evidence base and understanding.

Questions 30 and 31

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

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

Respondents were asked how effective they think the suggested measures will be in increasing the Government's ability to understand the ransomware threat to the UK, and in increasing their ability to tackle and respond to the ransomware threat to the UK. There were mixed responses across all measures. All new measures (Measures 2-5) were viewed as more effective than staying with the current regime (Measure 1).

'Measure 2: Economy-wide mandatory reporting for all organisations and individuals' had the highest level of perceived effectiveness across all measures. Around three quarters thinking this economy-wide measure would be effective in increasing the Government's ability to understand the ransomware threat to the UK (79% net effective) and effective in increasing the Government's ability to tackle and respond to the ransomware threat in the UK (74% net effective). This measure also had the highest proportion of respondents who responded that 'Measure 2' would be 'effective' in increasing the Government's ability to understand the ransomware threat to the UK (51%) and in increasing their ability to tackle and respond to the ransomware threat to the UK (44%).

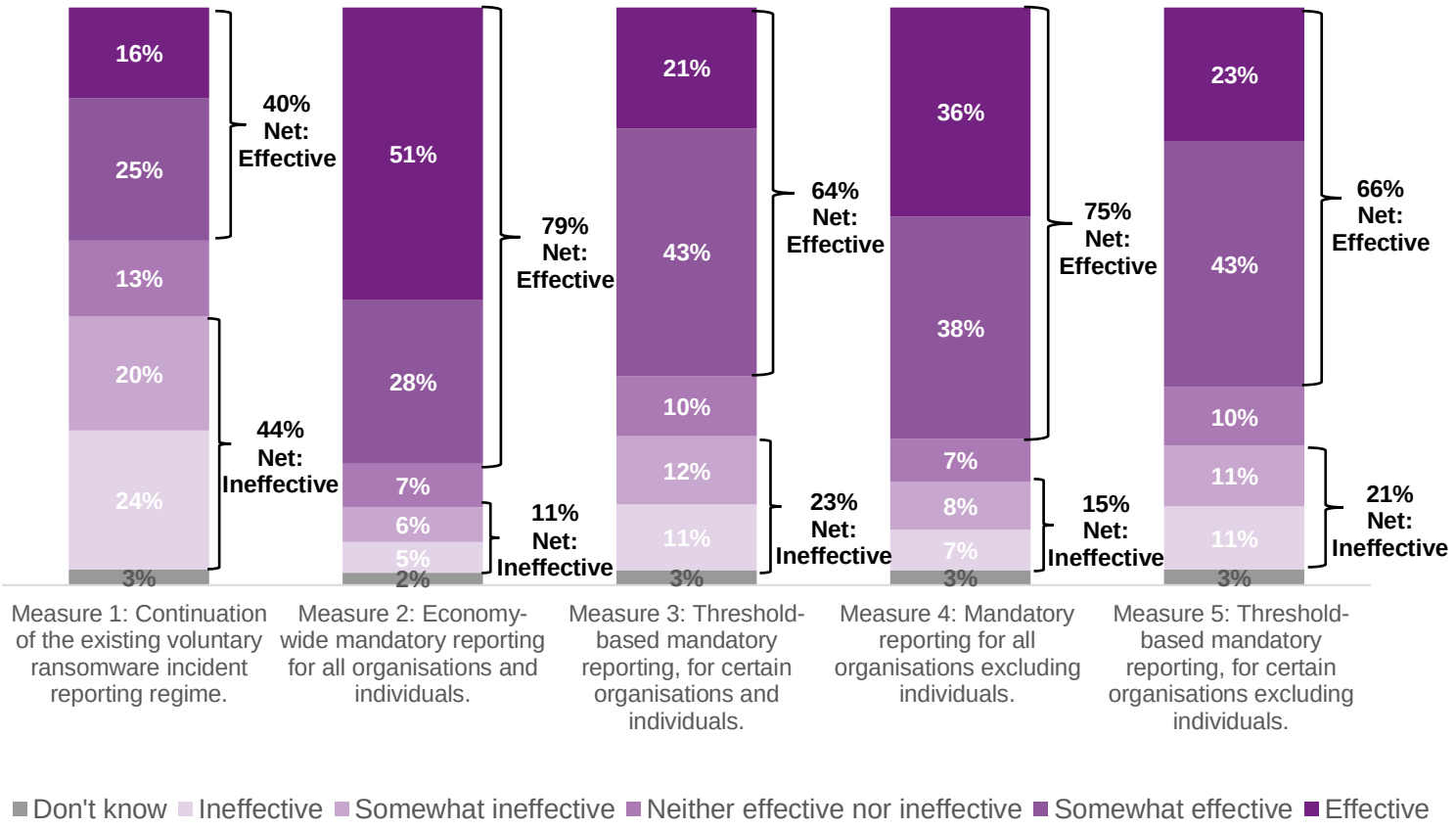
For this measure, both effectiveness in increasing understanding of the ransomware threat and effectiveness for increasing ability to tackle/respond to the threat, individuals thought it would be more effective than organisations.

'Measure 4: Mandatory reporting for all organisations excluding individuals' had the second highest proportion of respondents who responded it would be 'effective' in increasing understanding the ransomware threat (36%) and in increasing their ability to tackle/respond to the threat (31%).

Approximately a fifth of respondents thought that Measures 3 and 5 would be 'effective' in increasing the Government's ability to understand the threat to the UK (21% and 23% respectively) and increasing the Government's ability to tackle and respond to the ransomware threat to the UK (16% and 20% respectively).

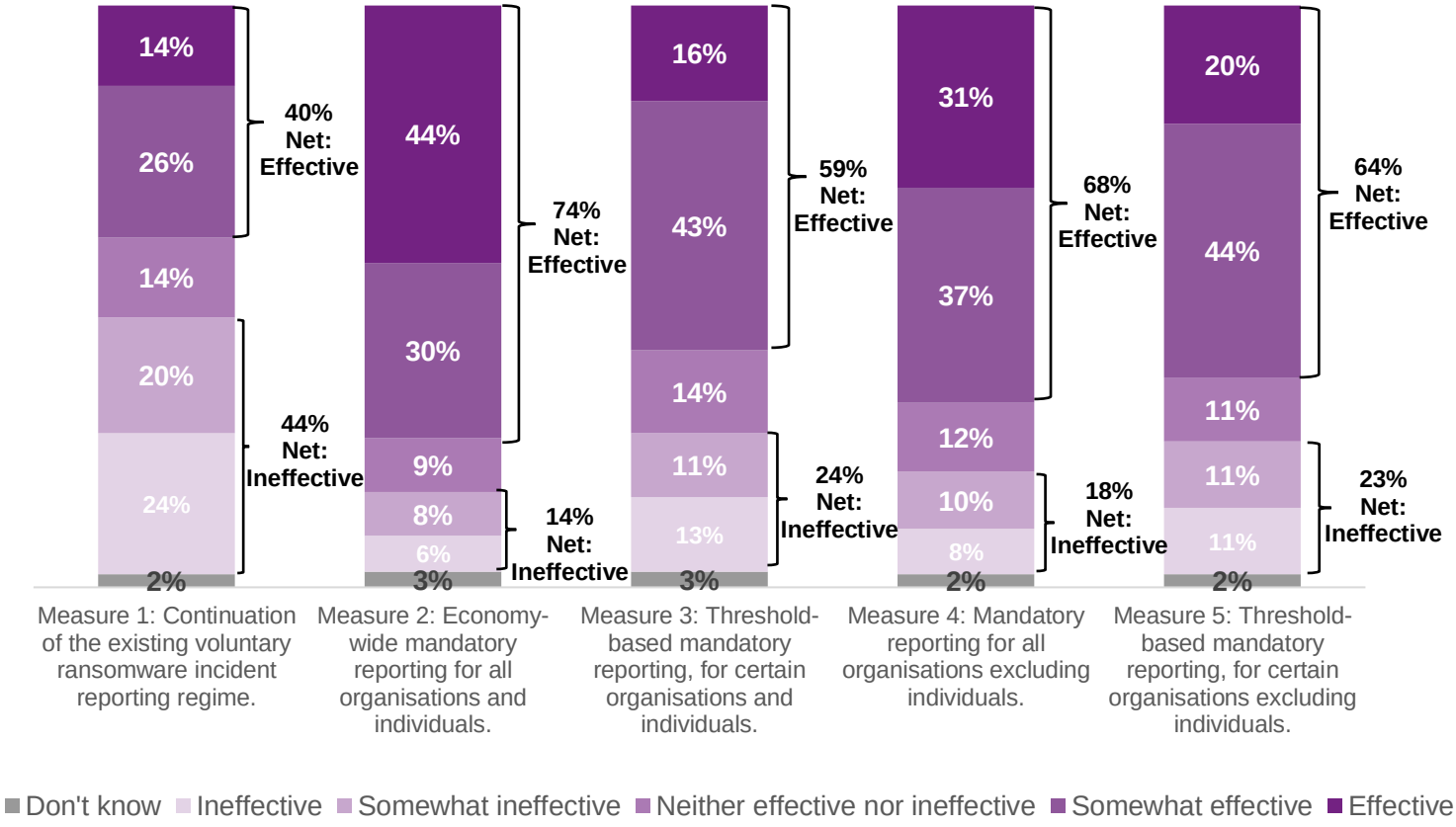
Respondents' views on 'Measure 1' had the highest proportion of respondents who thought that this measure would be ineffective for both increasing understanding and increasing ability to tackle/respond to the threat (44% net ineffective).

Figure 22: Perceived effectiveness of ransomware incident reporting regime for increasing the Government's ability to understand the ransomware threat to the UK



Q30: *How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK?.* ***Base*** *= All (Measure 1 and 5 n=228; Measures 2,3 and 4 n=229)*

Figure 23: Perceived effectiveness of ransomware incident reporting regime for increasing the Government's ability to tackle and respond to the ransomware threat to the UK



***Q31:** How effective do you think the following would be in increasing the Government's ability to tackle and respond to the ransomware threat to the UK?.* ***Base** = All (Measure 1 and 5 n=228; Measures 2,3 and 4 n=229)*

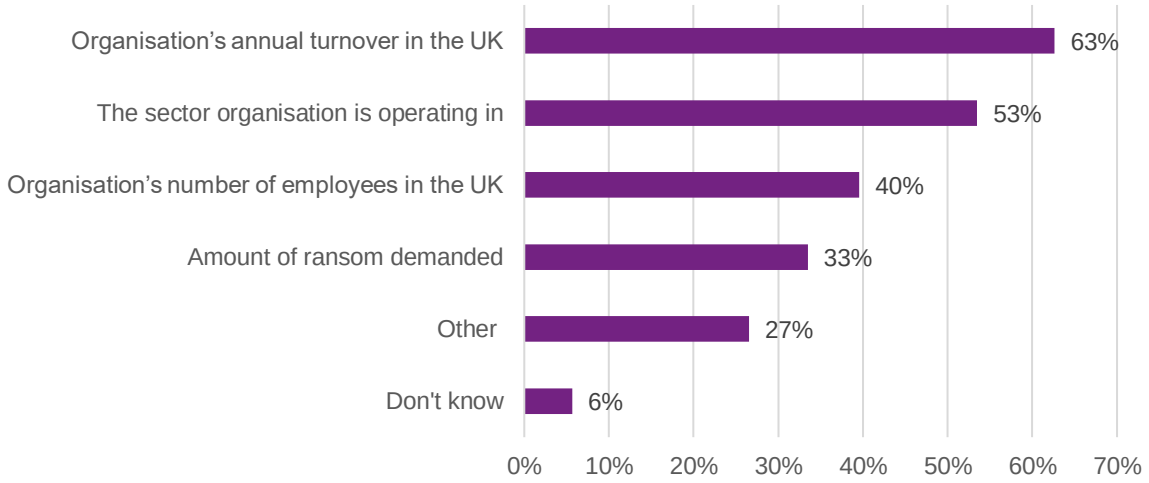
Question 32

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

Respondents could select multiple options for this question. They thought there were several key approaches to best determine the threshold for inclusion for a threshold-based payment prevention programme: by annual turnover in the UK (63%) and by sector (53%) had the highest proportion of respondents.

Four in ten respondents thought that an organisation's number of employees in the UK (40%) would be a good way to determine the threshold for inclusion and a third of respondents (33%) thought the amount or ransom demanded would be appropriate. Over a quarter (27%) responded 'Other' to identify different ways to determine the threshold for inclusion.

Figure 24: Respondents' views on the best way to determine the threshold for inclusion



Q32: *If we introduced a mandatory reporting regime for victims within a certain threshold, what would be the best way to determine the threshold for inclusion?* ***Base*** *= All (n=230)*

Respondents who selected 'Other' were able to provide additional information (n=55). Several respondents suggested that thresholds should be based on specific characteristics, including:

- Size of the organisation
- Annual global turnover
- Level of risk or importance to the UK economy or security
- Sector-specific thresholds

A small number of respondents suggested that thresholds should be based on the impact of the attack, such as any repercussions or harms caused, including on the victim and any wider impact on society.

A few respondents reflected in this section that they were against any thresholds or mandatory reporting, for example:

> *"There should be no threshold to reporting. Putting this in place will only shift the ransomware risk towards those less able to deal with it."* ***– Individual Respondent***

Prose respondents provided comments on having thresholds for mandatory reporting, these included thresholds based on organisation size and amount of ransom demanded. Other suggestions included a tiered reporting structure for CNI organisations and reducing the amount of detail needed from small organisations.

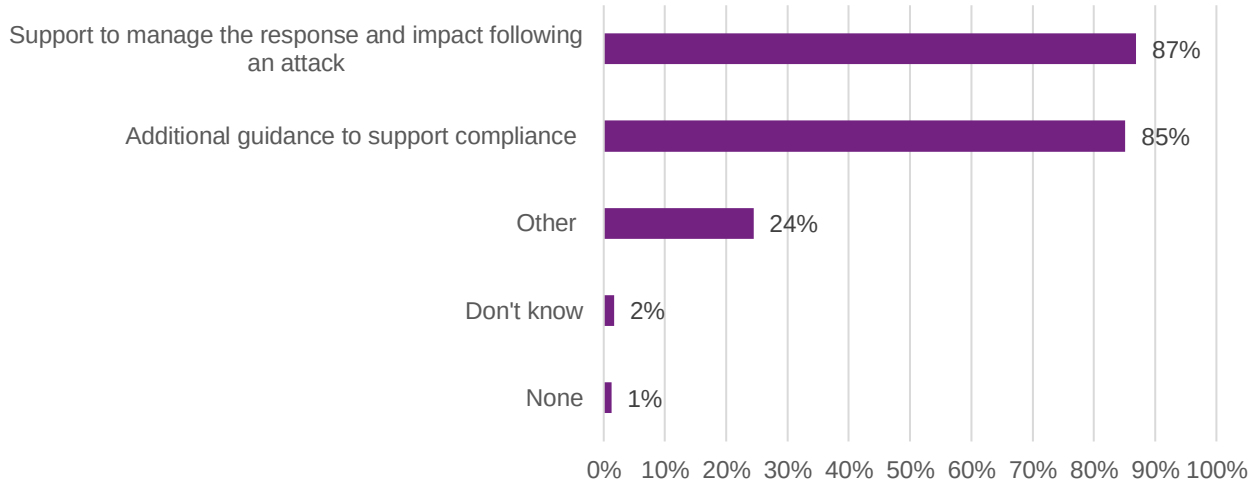
Prose respondents also addressed the need to focus on actual ransomware attacks rather than suspected attacks to prevent overreporting and efficiently use resources.

Question 33

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

Respondents were able to select more than one option for this question. The majority thought that support to manage the response and impact following an attack would aid compliance with a mandatory reporting regime (87%), as would additional guidance (85%).

Figure 25: Respondents' views on what measures would aid compliance with a mandatory reporting regime



Q33: *What measures do you think would aid compliance with a mandatory reporting regime?* ***Base*** *= All (n=229)*

Nearly a quarter of respondents (24%) responded 'Other' to identify different measures to support compliance. These respondents were able to provide additional information (n=51).

Many respondents provided further information about support measures to aid compliance. This addressed:

- Training and education e.g. better advertising of the reporting process, robust guidance on reporting, and building awareness through communication campaigns
- Improving cyber resilience e.g. compulsory cyber insurance, independent technical expertise, better cyber security provisions, resilience building, and aligning mandatory reporting with improved cyber security regulations
- Incident and recovery support e.g. during and after attacks, implementing statutory standards for businesses continuity and disaster recovery practices

"The implementation of mandatory reporting requirements for ransomware incidents will necessitate significant investment in both human and technological resources." ***– Organisation Respondent***

A few respondents believed that introducing consequences and penalties for non-compliance would aid compliance and encourage reporting.

Respondents also provided other additional information on aiding compliance with a mandatory reporting regime, including:

- Encouraging support from wider industry, e.g. from larger IT organisations and from legal and insurance systems
- Having a phased introduction or tailored measures e.g. sector specific
- The inclusion of confidentiality measures, e.g. anonymous reporting and intelligence and information sharing
- Ensuring there is a streamlined process, including coordinating with existing regulation or compliance requirements and introducing accountability and transparency measures

Those that responded 'None' were able to provide further information. Views did not support these compliance options and more generally did not support a mandatory reporting regime.

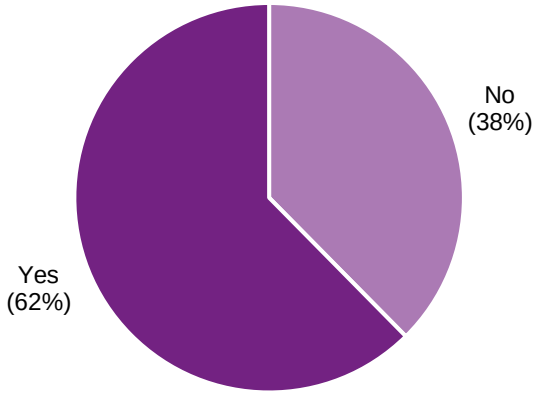
Additional prose responses suggested other compliance measures, such as introducing tax relief incentives for organisations meeting reporting requirements or adopting comprehensive cyber insurance policies and improved public education on cyber risks and mitigation.

Question 34

Q34: Do you think these compliance measures need to be tailored for different organisations or individuals?

Around six in ten respondents (62%) thought that compliance measures need to be tailored for different organisations or individuals. Just over a third (38%) did not think they need to be.

Figure 26: Respondents' views on whether compliance measures need to be tailored



Q34: *Do you think these compliance measures need to be tailored for different organisations or individuals?* ***Base*** *= All (n=226)*

Respondents that selected 'Yes' could provide more details on how they thought measures should be tailored and to suggest any alternative measures (n=85).

A small majority of respondents thought that compliance measures should be tailored based on specific characteristics. This included sector type, size of organisation, the technology organisations have available, or whether the organisation is international.

A few respondents thought that there should be clearer reporting processes and guidance. For example, improving existing systems, making processes more specific, and incentivising reporting.

> *"There needs to be different routes for reporting as an organisation and reporting as an individual. Telling people to report to "Action Fraud" is confusing as it's not what people think of as fraud so having a specific channel for reporting for individuals and reporting for businesses would be helpful."* ***– Individual Respondent***

A few respondents thought that there should be separate policies for individuals and organisations. For example, a sliding scale of penalties based on sector type, turnover, number of employees, organisation size, and because individuals potentially do not have the same awareness of reporting tools as organisations.

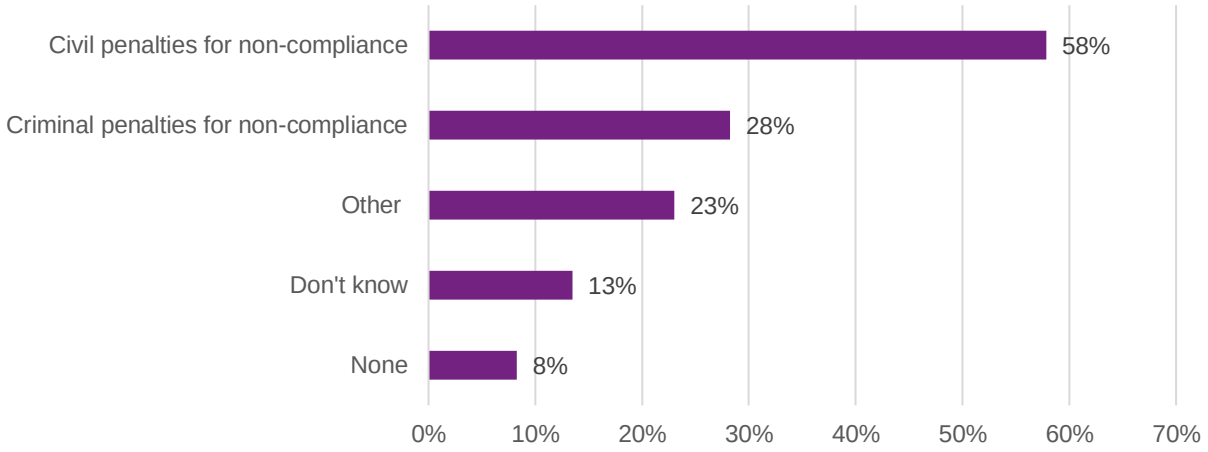
Question 35

Q35: What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime?

For this question, respondents could select multiple options. Around six in ten (58%) thought that civil penalties would be appropriate for non-compliance with a mandatory reporting regime and just over a quarter (28%) thought that criminal penalties would be. Nearly a quarter (23%) responded that 'Other' measures would be appropriate for this.

A minority (8%) thought that there would be no appropriate non-compliance measures.

Figure 27: Respondents' views on what measures would be appropriate for managing non-compliance with a mandatory reporting regime



Q35: *What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime?*
Base *= All (n=230)*

Respondents who selected 'Other' were able to provide additional information (n=52). Many respondents provided more information on appropriate measures to support and encourage compliance rather than punish non-compliance.

Many respondents expressed further views that the use of penalties would serve as an appropriate measure for non-compliance with a mandatory reporting regime. This included criminal penalties, sanctions, public reprimands, and financial penalties.

Several respondents thought that penalties should be tailored, such as on thresholds or tiers, consequences for seniors, and graduated enforcement.

> *"Civil penalties for organisations. Criminal penalties for individuals - but education should be the first step."* ***– Organisation Respondent***

A small portion of respondents identified potential issues with non-compliance measures. For example, costs for managing non-compliance outweighing any benefits, risk it will discourage transparency and reporting, and that penalties will revictimise.

> *"Transparency and open communication are crucial for understanding the threat landscape and developing effective countermeasures. Encouraging organisations to report incidents without the fear of punishment is essential for a collaborative approach to cybersecurity."* ***– Organisation Respondent***

Those that responded 'None' were able to provide further information. Many of these respondents identified similar issues as the free-text responses for 'Other' non-compliance measures. Furthermore, the majority of these respondents also advocated for encouraging reporting and cyber security measures instead of non-compliance measures.

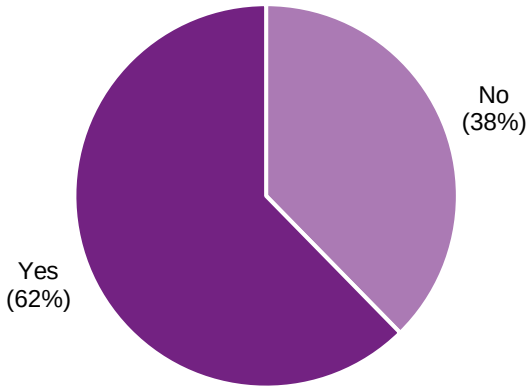
Prose respondents commented that there needed to be consideration of where investigative responsibilities lie for non-compliance enforcement and what the implications would be if non-compliance is identified months or years after an attack.

Question 36

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

Nearly two thirds of respondents (62%) thought that non-compliance measures need to be tailored for different organisations and individuals with just over one third (38%) who thought they do not need to be.

Figure 28: Respondents' views on whether non-compliance measures need to be tailored



Q36: *Do you think these non-compliance measures need to be tailored for different organisations and individuals?* ***Base*** *= All (n=223)*

Respondents that selected 'Yes' could provide more details on how they thought measures should be tailored and to suggest any alternative measures (n=69).

Most respondents provided a wide range of suggestions on how non-compliance measures could be tailored. This included:

- Size of organisation
- Whether the organisation is in the public or private sector
- Available resources
- Impact of the attack

"Non-compliance measures should be tailored to reflect the size, resources, and circumstances of organisations and individuals…Tailoring measures ensures fairness and encourages participation while maintaining the regime's effectiveness." ***– Organisation Respondent***

A few respondents thought that individuals should be excluded from any non-compliance measures. Reasons included, individuals' lack of resources and capacity, that individuals are less likely to be aware of the requirement, or of how to report the attack; and the risk of revictimisation.

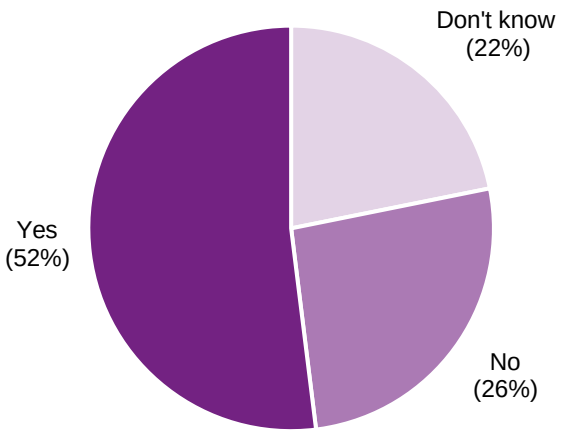
A few respondents also suggested the requirement for clear education and guidance to aid compliance and incentivise reporting, instead of having non-compliance measures.

Question 37

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

Just over half of respondents (52%) thought that the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors. Just over a quarter (26%) thought this will not have an impact and nearly a quarter (22%) did not know if there would be an impact.

Figure 29: Respondents' views on whether the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors



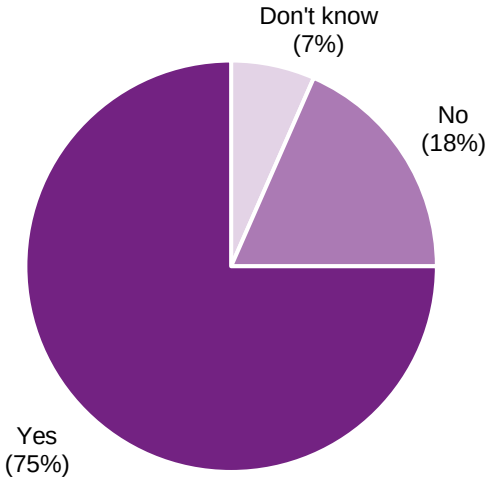
Q37: *Do you think the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors?* ***Base*** *= All (n=229)*

Question 38

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

Three quarters of respondents (75%) thought that 72 hours was a reasonable timeframe for a suspected ransomware victim to make an initial report of an incident. Nearly a fifth of respondents (18%) did not think this was a reasonable timeframe.

Figure 30: Respondents' views on whether 72 hours is a reasonable timeframe for a suspected ransomware victim to make an initial report



Q38: *For the mandatory reporting regime, is 72 hours a reasonable time frame for a suspected ransomware victim to make an initial report of an incident?* ***Base*** *= All (n=228)*

Those that responded 'No' were able to provide further information on their response (n=36). Nearly all respondents thought that there should be more than 72 hours allowed to report a ransomware incident. Respondents did not believe it would be enough time to report. Some suggestions included 5-7 days to report.

Many respondents thought that it would be helpful to have flexible timelines dependent on an organisation's resources, scope, or size.

> *"A flexible timeline would have to be implemented. SME's might take longer to report due to staffing issues or lack of security staff etc, whilst larger organisations can reply within that 72 hours. Other companies might need longer depending on the size of their security teams or other compliance issues they might face."* ***– Individual Respondent***

A few respondents thought that reporting was not a priority in an attack. They thought that the focus should be on containing and ending the incident while an attack is occurring and that submitting a more detailed report after the attack would be useful.

> *"Short periods are better to assist [the] response but some organisations may not even identify that they need to report as [if] this is their first major attack, [they] don't understand what is happening."* ***– Individual Respondent***

A minority of these respondents thought that ransomware victims should report an incident within less than 24 hours.

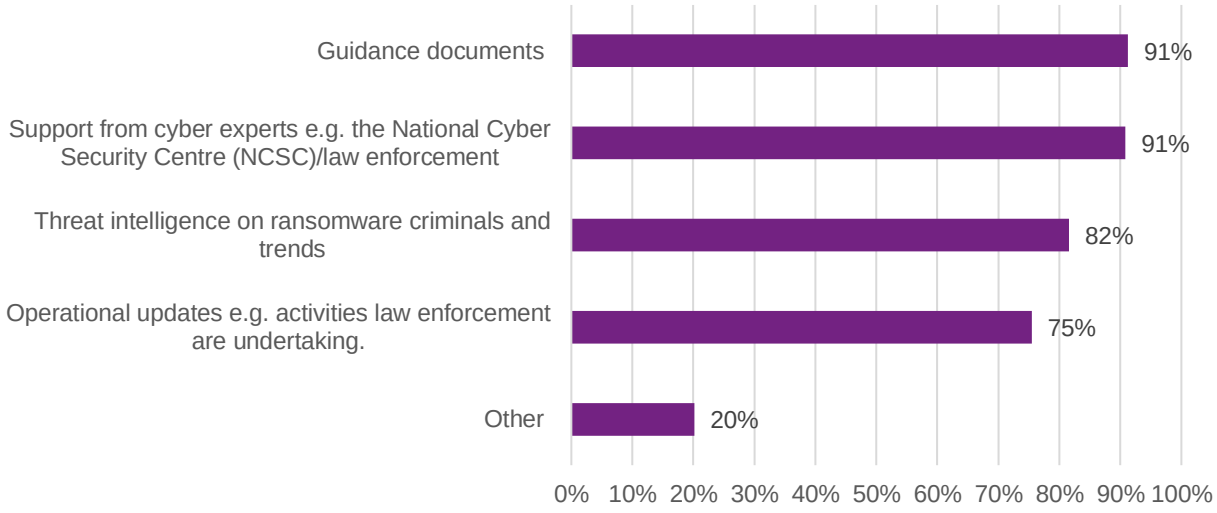
Question 39

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

Respondents were able to select more than one option for this question. Most respondents thought that there should be a variety of services offered to victims when reporting. Around nine in ten thought that guidance documents and support from cyber experts for example, the National Cyber Security Centre (NCSC) or law enforcement (both 91%), should be provided. Threat intelligence on ransomware criminals, trends, and operational updates were also selected by many respondents (82% and 75% respectively).

A fifth of respondents (20%) thought that there were 'Other' services that should be provided.

Figure 31: Respondents' views on the services to victims that should be offered by an incident reporting regime



Q39: *Do you think that an incident reporting regime should offer any of the following services to victims when reporting?*
Base *= All (n=228)*

Those that selected 'Other' could provide further information (n=44). Several respondents suggested that threat intelligence on ransomware attacks should be shared, such as public reports on cyber incidents.

A notable portion of respondents thought that guidance and assistance should be offered to ransomware victims. Suggestions included guidance on managing data breaches, assistance with recovery planning, and decryption technology.

> *"An incident reporting scheme should provide all of the following: support from cyber experts, guidance documents, threat intelligence on ransomware criminals and trends, operational updates. This could ensure that victims can be supported during reporting."* ***– Organisation Respondent***

Several respondents also wanted more support including from cyber experts, financial support on preventative measures, and Government support for charities. A small portion of respondents specifically wanted more industry support and coordination with the ICO and regulators.

Respondents also suggested other services, such as confidential reporting, clear definitions, and incentivised reporting. A few respondents wanted any measures to be tailored and advocated for proportionality.

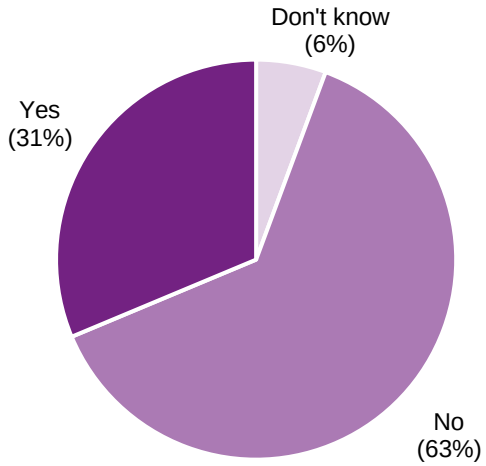
These views were echoed by prose respondents who also agreed that further guidance on the reporting regime was needed, offering services to support victims, and advice from cyber experts.

Question 40

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

Nearly two thirds of respondents (63%) thought that mandatory reporting should not cover all cyber incidents (including phishing, hacking etc.), rather than just ransomware, with nearly a third (31%) who thought it should cover all cyber incidents.

Figure 32: Respondents' views on whether mandatory reporting should cover all cyber incidents



Q40: *Should mandatory reporting cover all cyber incidents (including phishing, hacking etc.), rather than just ransomware)* ***Base*** *= All (n=230)*

Government policy response

Overall, the consultation responses demonstrated strong support for the implementation of a new mandatory reporting system. All four new measures that were outlined to respondents were viewed more favourably than maintaining the status quo of a current voluntary reporting system. Measures 2-5 all had higher agreement levels amongst respondents than maintaining the current voluntary system. Responses were therefore in

favour of implementing a new mandatory system. The Government will continue to develop this proposal.

Further work will be conducted to determine the scope and whether any requirements should be based on a threshold, as well as appropriate and proportionate penalties for non-compliance. Detailed guidance will be published ahead of any new reporting requirements coming into force.

Of the four measures, 'Measure 2' (economy-wide mandatory reporting for all organisation and individuals) was the preference of respondents. Feedback indicated strong support for 'Measure 2', with 79% of respondents thinking that the measure would be net effective in increasing the Government's ability to understand the ransomware threat to the UK. A further 74% thought that the measure will be net effective in increasing the Government's ability to tackle and respond to the ransomware threat to the UK. Measure 2 also had the highest proportion of agreement to implement (63% net agreement) whereas less than half agreed (41% net agreement) with the continuation of the existing voluntary ransomware incident reporting mechanism by itself.

Some respondents believed individuals should be excluded from the mandatory reporting regime as they felt it could be unrealistic to expect individuals to comply with the reporting requirements. Some responses indicated that a threshold approach may be more suitable. Additional suggestions for thresholds for inclusion were as follows: based on the size of the organisation; by annual global turnover; sector specific thresholds or by the level of risk/importance to the UK economy and security. The Government will continue to consider this feedback and will provide further clarity on the scope of the mandatory reporting regime.

Most respondents agreed that there would be a need for additional measures to aid compliance with a mandatory reporting regime, including 87% feeling that support in managing the response and impact following an attack would be helpful, and 85% believing additional guidance to support compliance would be welcomed. The Government will consider this feedback and provide accompanying guidance ahead of new reporting requirements coming into force.

Around half of respondents thought civil penalties would be appropriate for non-compliance (vs 28% for criminal penalties), but it was acknowledged by respondents that this should be tailored for different organisations and individuals. The Government will continue to consider appropriate and proportionate penalties.

Three-quarters of respondents thought that 72 hours was a reasonable timeframe for a suspected ransomware victim to make an initial report of the incident. Therefore, the Government will keep 72 hours as the suggested reporting timeframe. There was a strong feeling among respondents towards several additional support measures that should be made available to victims, including guidance documents, NCSC/law enforcement support, threat intelligence support on ransomware criminals/trends and operational updates from

law enforcement. The Government will continue to work with operational partners to consider an appropriate and proportionate package for victim support.

Additional Comments

Analysis summary

Question 41

Q41: Do you have any other comments on our consultation proposals?

Two fifths of respondents (40%) said they did have additional comments on the consultation proposals. There was a wide range of additional comments reported which have been read and considered.

Reflections on the suggested legislative measures included:

- Expanding the legislation to include other cyber crime, small businesses, and the supply chain
- Financial penalties for non-compliance
- UK being an international lead on ransomware policy

Respondents also raised further concerns about compliance, measures encouraging perpetrators to shift targets, and the risk of criminalising victims.

Respondents proposed a variety of additional suggestions and considerations. Examples include:

- Strengthening organisation and individual capabilities, such as recovery and back-up measures and cyber security training
- Consideration of attacks that do not have financial motivation
- Consultation with industry experts
- Financial incentives for good cyber security culture
- Improving clarity on definitions and thresholds for legislative options

Additional prose responses also identified further considerations, such as views on the role and impact of these proposals on cyber insurance and aligning with international initiatives.

Question 42

Q42: Do you have any data or evidence to demonstrate:

- **the scale of ransomware impacting the UK?**
- **the cost of ransomware to the economy or specific businesses when either a ransom has been paid or has not?**
- **the impact of a targeted ban on ransomware payments for critical national infrastructure (CNI) owners and operators (who are regulated/ have competent authorities), and the public sector, including local government?**
- **the impact of either an economy wide or threshold-based ransomware payment prevention regime?**
- **the impact of either an economy wide or threshold based mandatory ransomware incident reporting regime?**

Respondents were asked if they had any data or evidence to address any further understanding on the ransomware threat (n=50).

Additional perceptions and comments were provided on the scale and cost of the ransomware threat, and the impact on CNI sectors, as well as suggestions of articles and additional data sources. These responses and sources have been read and considered.

Question 43

Q43: Are you aware of any impact the proposals may have that we have not captured in the consultation options assessment, published alongside this document?

Respondents were asked if they were aware of any impact the proposals may have that have not been captured on the consultation options assessment published alongside the consultation (n=56).

There was a wide range of potential impacts reported. For example, concerns about costs, such as resources required or knock on effects to businesses, ransomware actors shifting their targets to other countries or new strategies, impact on the cyber insurance market, and impacts on SMEs. Some responses also identified the need for more research on the area, including sector specific to assess the impact of these proposals. All responses have been read and will be considered in future work.

Impact Assessment, Equalities and Welsh Language

Equality Impact Assessment

Section 1 - Name and outline of policy proposal, guidance, or operational activity

Title: Ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting.

The Home Office has three immediate, overarching objectives when it comes to our work in this area:

- 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.

The key aim of these proposals is to protect UK businesses, citizens and CNI, whether UK owned or not.

The overriding strategic objective of the proposed interventions is to reduce cyber crime and the associated harms to UK businesses and the public, 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.

Section 2 - Summary of the evidence considered in demonstrating due regard to the Public-Sector Equality Duty (PSED).

The Government ran a public consultation between January and April 2025. During the consultation process, the Government received 273 responses, of which 233 were via the online survey or followed the survey format. A further 40 responses took other forms such as emails or written prose. Alongside formal responses, the Government held 36 events to encourage engagement in the consultation process. Respondents to the consultation included a mix of organisations (57%) and individuals (39%). Individuals were asked to confirm their age range, gender, ethnicity and in which part of the UK they resided.

There is no evidence that the risk of exploitation of individuals from a ransomware attack would be higher than in other crimes. There is limited evidence available when having due

regard for public sector equality in relation to the consultation proposals. The Home Office believe that this will not have a discriminatory effect against anyone with protected characteristics.

Overall, the Home Office believe the benefits of these proposals 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 will be positively impacted through reduced criminality. In developing the proposals post consultation, the Home Office is taking into account consultation responses, to ensure all impacts on the public are considered and all possible and proportionate mitigations are taken.

Section 3 - Consideration of duty

3a. Consideration of limb 1 of the duty: Eliminate unlawful discrimination, harassment, victimisation, and any other conduct prohibited by the Equality Act.

Age

Direct Discrimination: None identified.

Indirect Discrimination: The reporting regimes will require that victims of a ransomware incident report details about their proposed payment or details about the incident to a reporting platform. The reporting platform will be online and there could be a potential difficulty with elderly persons using the online reporting services. An alternative mechanism will be available to ensure that reports can be made offline, where necessary.

Disability

Direct Discrimination: None identified.

Indirect Discrimination: The reporting regimes will require that victims of a ransomware incident report details about their proposed payment or details about the incident to a reporting platform. The reporting platform will be online and there could be a potential difficulty for person with a disability in using the online reporting services. An alternative mechanism will be available to ensure that reports can be made offline, where necessary.

Gender Reassignment

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Marriage and Civil Partnership

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Pregnancy and Maternity

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Race

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Religion or Belief

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Sex

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

Sexual Orientation

Direct Discrimination: None identified.

Indirect Discrimination: None identified.

3b. Consideration of limb 2: Advance equality of opportunity between people who share a protected characteristic and people who do not share it.

Under paragraph 2(1) of Schedule 18 to the Equality Act 2010, the requirement under section 149(1)(b) to advance equality of opportunity between those who have a relevant protected characteristic and those who do not, does not have to be considered in relation to the exercise of immigration and nationality functions in respect of age, race, religion or belief, where race relates to nationality or ethnic or national origins. This leaves a limited number of protected characteristics to be considered under limb 2: disability, gender re-assignment, pregnancy and maternity, race (colour), sex and sexual orientation.

Age

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Disability

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Gender Reassignment

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Maternity and Pregnancy

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Race

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Religion or Belief

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Sex

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

Sexual Orientation

There is no evidence to suggest the legislative proposals affect the equality of opportunity between people who share this protected characteristic and people who do not share it.

3c. Consideration of limb 3: Foster good relations between people who share a protected characteristic and persons who do not share it.

Age

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Disability

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Gender Reassignment

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Maternity and Pregnancy

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between

groups with this protected characteristic and those who do not, whether directly or indirectly.

Race

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Religion or Belief

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Sex

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Sexual Orientation

The legislative proposals are not being created to help to tackle prejudice and promote understanding. It will not be used to help build or enable better relationships between groups with this protected characteristic and those who do not, whether directly or indirectly.

Section 4 - Community Considerations

The ransomware legislative proposals are unlikely to have a specific impact on communities in the UK. There is the potential for it to impact (disrupt) communities of criminals.

Section 5 - Summary of foreseeable impacts of policy proposal, guidance or operational activity on people who share protected characteristics

Protected Characteristic Group	Potential for Positive or Negative Impact?	Explanation	Action to address negative impact
Age	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Disability	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Gender Reassignment	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Marriage and Civil Partnership	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Pregnancy and Maternity	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Race	Neutral	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Religion or Belief	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Sex	Neutral.	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	
Sexual Orientation	Neutral	The legislative proposals are not expected to have an impact on this characteristic. They aim to make the UK safer for individuals and organisations, from online cyber criminals.	

Section 6 - In light of the overall policy objective, are there any ways to avoid or mitigate any of the negative impacts that you have identified above?

We will be providing alternative, accessible ways to report through the reporting regimes (i.e. a telephone number) and will undertake a comprehensive comms campaign to ensure wide awareness of the policy.

Section 7 – Review date:

11/07/2025

Section 8 - Declaration

I have read the available evidence, and I am satisfied that this demonstrates compliance, where relevant, with Section 149 of the Equality Act and that due regard has been made to the need to: eliminate unlawful discrimination; advance equality of opportunity; and foster good relations.

SCS sign off:
John Evans, Cyber Policy Unit Head
Name/Title: Ransomware legislative proposals
Directorate/Unit: Directorate of State Threats and Cyber, Cyber Policy Unit
Lead contact: Charlie Smoothy
Date: 11/07/2025

For monitoring purposes all completed EIA documents and updated EIAs (Equality Impact Assessment) **must** be sent to the PSED@homeoffice.gov.uk

Date sent to PSED Team:
11/07/2025

Equalities

Instructions: The Public sector Equality Duty came in to force in April 2011 and public authorities including Home Office are now required to have due regard to the need to achieve the objectives set out under s149 of the Equality Act 2010 to:

(a) eliminating discrimination, harassment, victimisation and any other conduct that is prohibited by or under the Equality Act 2010;
(b) advancing equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it;
(c) fostering good relations between persons who share a relevant protected characteristic and persons who do not share it.

The proportionate Equality Analysis that accompanied the consultation should now be updated in light of the consultation responses to consider likely impacts on people with protected characteristics: disability, race, sex, gender reassignment, age, religion or belief, sexual orientation, pregnancy and maternity, marriage and civil partnership.

Any new points raised in relation to equalities impacts from the policy proposals should be proportionately responded to. Any new evidence supplied should also be considered to be sure the policy intentions are likely to still be achieved for people with protected characteristics. If there are mitigations suggested by consultees these should also be considered.

More information on the PSED can be found here:
https://www.gov.uk/government/organisations/home-office/about/equality-and-diversity

Welsh Language Impact Test

[Instructions: In accordance with the Welsh Language Act 1993, the Home Office's Welsh Language Scheme, requires you to 'assess the linguistic consequences of policies affecting services provided to the people in Wales'. The following areas will need to be considered in the light of responses to the consultation exercise.]

- Were there any responses from Welsh stakeholders that raised particular issues or considerations for Wales or Welsh-speakers that need responding to?

- No.

- If yes, have you assessed the likely impacts on service delivery of the policy proposals on the use of the Welsh language in Wales?

- What action have you taken to ensure that the policy proposals are consistent with the requirements set out in the Home Office Welsh Language Scheme? (e.g. have you considered having a Welsh language translation of the consultation response?)

- We translated the consultation document into Welsh, and we will translate this document into Welsh.

Further guidance can be found here: https://www.gov.uk/government/organisations/home-office/about/welsh-language-scheme

Consultation principles

The principles that Government departments and other public bodies should adopt for engaging stakeholders when developing policy and legislation are set out in the Cabinet Office Consultation Principles 2018:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Annex A – Consultation Questions

Section 1: Background questions

This section seeks information on you or your organisation. It will be used to check that we have received responses from across our target audiences and help us to consider different personal and organisational views.

Q1. Are you responding to this survey as an individual or as a representative of an organisation? *Please select one.*

1 ☐ Individual → Go to Q2

2 ☐ Organisation → Go to Q5

98 ☐ Other, *please specify [free text]* _____

Q2. [IF INDIVIDUAL] What is your age? *Please select one option.*

1 ☐ Under 18
2 ☐ 18-24
3 ☐ 25-34
4 ☐ 35-44
5 ☐ 45-54
6 ☐ 55-64
7 ☐ 65+
97 ☐ Prefer not to say.

Q3. [IF INDIVIDUAL] What is your gender? *Please select one option.*

1 ☐ Female
2 ☐ Male
98 ☐ Other, please specify *[free text]* _____
97 ☐ Prefer not to say.

Q4. [IF INDIVIDUAL] What is your ethnicity? *Please select one option.*

1 ☐ Asian or Asian British,
2 ☐ Black, Black British, Caribbean or African
3 ☐ Mixed or multiple ethnic groups
4 ☐ White
98 ☐ Other ethnic group, please specify *[free text box]* _____
97 ☐ Prefer not to say.

Q5. [ALL] Which of the following options best describes the sector you work in? *If you are responding on behalf of an organisation, please select the sector of the organisation.*

1 ☐ Academia
2 ☐ Business/Industry
3 ☐ Central Government/Civil Service
4 ☐ Law Enforcement
5 ☐ Legal
6 ☐ Local Government

7 ☐ Third Sector/Voluntary
8 ☐ Critical National Infrastructure (CNI) → Go to Q6
9 ☐ Other Public Service/Public Body
98 ☐ Other, please specify *[free text]*
97 ☐ Prefer not to say.

Q6. [IF CNI] Which of the following options best describes the sector of your organisation? *Please select one option.*

1 ☐ Chemicals
2 ☐ Civil Nuclear
3 ☐ Communications
4 ☐ Defence
5 ☐ Emergency Services
6 ☐ Energy
7 ☐ Finance
8 ☐ Food
9 ☐ Government
10 ☐ Health
11 ☐ Space
12 ☐ Transport
13 ☐ Water
97 ☐ Prefer not to say.

Q7. [IF AN ORGANISATION] How many people work for your organisation across the UK as a whole?

1 ☐ Under 10
2 ☐ 10–49
3 ☐ 50–249
4 ☐ 250 +
99 ☐ Don't know.
97 ☐ Prefer not to say.

Q8. [IF AN ORGANISATION] What is your organisation's annual turnover?

1 ☐ 0-£49,000
2 ☐ £50,000 - £99,000
3 ☐ £100,000 - £249,000
4 ☐ £250,000 - £499,000
5 ☐ £500,000 - £999,000
6 ☐ £1,000,000 - £1,999,000
7 ☐ £2,000,000 - £4,999,999
8 ☐ £5,000,000 - £9,999,999
9 ☐ £10,000,000 - £49,999,999
10 ☐ £50,000,000 or more
99 ☐ Don't know.
97 ☐ Prefer not to say.

Q9. [ALL] What part of the UK are you based in? *If you are responding on behalf of an organisation, please select where your organisation is mainly based.*

1 ☐ England
2 ☐ Wales
3 ☐ Scotland
4 ☐ Northern Ireland
5 ☐ I am not based in the UK.
97 ☐ Prefer not to say.

Section 2: Proposal 1 - Targeted ban on ransomware payments

- **A ban on ransomware payments for all public sector bodies, including local government, and for owners and operators of Critical National Infrastructure** (that are regulated, or that have competent authorities)**.**

Scope outline
The questions below are largely directed at those CNI owners and operators (who are regulated/have competent authorities) and the public sector, including local government, but we also welcome responses from others who have an interest in these sectors.
Please find the relevant information on **Proposal 1: Targeted ban on ransomware payment** in paragraphs 43-49 and Figure 2 in this consultation document.

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

1 ☐ Strongly agree.
2 ☐ Tend to agree.
3 ☐ Neither agree nor disagree.
4 ☐ Tend to disagree.
5 ☐ Strongly disagree.
99 ☐ Don't know.

Please provide any further explanation for your response [free text]:

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

1 ☐ Effective
2 ☐ Somewhat effective
3 ☐ Neither effective nor ineffective
4 ☐ Somewhat ineffective
5 ☐ Ineffective
99 ☐ Don't know.

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

1 ☐ Effective
2 ☐ Somewhat effective
3 ☐ Neither effective nor ineffective
4 ☐ Somewhat ineffective
5 ☐ Ineffective
99 ☐ Don't know.

Q13. What measures do you think would aid compliance with the proposed ban? *Select all that apply.*

1 ☐ Additional guidance to support compliance with the ban.

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

98 ☐ Other, please specify *[free text]*

96 ☐ *None [free text]*

99 ☐ *Don't know.*

Q14. What measures do you think are appropriate for non-compliance with the proposed ban? *Select all that apply.*

1 ☐ Criminal penalties for non-compliance

2 ☐ Civil penalties for non-compliance

98 ☐ Other, please specify *[free text]*

96 ☐ None *[free text]*

99 ☐ *Don't know.*

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

1 ☐ Yes
2 ☐ No
99 ☐ Don't know.
100 ☐ Not applicable

If yes, what support would you need? [free text]:

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

1 ☐ Yes, please provide details *[free text]*
2 ☐ No, please provide details *[free text]*
99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No
99 ☐ Don't know.

If yes, please provide *further explanation for your response? [free text]:*

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

1 ☐ Yes widen the ban.
2 ☐ Yes impose a complete ban economy-wide.
3 ☐ No
99 ☐ Don't know.

If yes widen the ban, please provide further explanation for your response [free text]:

Section 3: Proposal 2 – A new ransomware payment prevention regime

- **A new ransomware payment prevention regime** to cover all potential ransomware payments from the UK.

Please find the relevant information on **Proposal 2: A ransomware payment prevention regime** in paragraphs 50-62 and Figure 3 in this consultation document.

Q19. To what extent do you agree, or disagree, that the Home Office should implement the following (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	**Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Strongly agree				
2 Tend to agree				
3 Neither agree nor disagree				
4 Tend to disagree				
5 Strongly				

disagree				
99 Don't know				

Please provide any further explanation for your responses *[free text] (optional):*

Q20. How effective do you think the following will be in reducing ransomware payments? (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	**Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g.* based on the size of the organisation and/or amount of ransom demanded.
1 Effective				
2 Somewhat effective				
3 Neither effective nor ineffective				
4 Somewhat ineffective				
5 Ineffective				
99 Don't know				

Q21. How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors? (please mark your response with an X in each column):

	Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.	**Threshold-based payment prevention regime, for certain organisations and individuals not covered by the ban set out in Proposal 1.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Payment prevention regime for all organisations not covered by the ban set out in Proposal 1 but excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based payment prevention regime for certain organisations not covered by the ban set out in Proposal 1, excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g.* based on the size of the organisation and/or amount of ransom demanded.
1 Effective				
2 Somewhat effective				
3 Neither effective nor ineffective				
4 Somewhat ineffective				
5 Ineffective				
99 Don't know				

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

1 ☐ Organisation's annual turnover in the UK
2 ☐ Organisation's number of employees in the UK
3 ☐ The sector the organisation is operating in.
4 ☐ Amount of ransom demanded.

98 ☐ Other, please specify *[free text]* _____

99 ☐ *Don't know.*

Q23. What measures do you think would aid compliance with a payment prevention regime? *Please select all that apply.*

1 ☐ Additional guidance to support compliance.

2 ☐ Support to manage the response and impact following an attack.

98 ☐ Other, please specify *[free text]*

96 ☐ None *[free text]*

99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No

If yes, please provide more details on how you think they should be tailored to different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

Q25. What measures do you think are appropriate for managing non-compliance with a payment prevention regime? *Please select all that apply.*

1 ☐ Criminal penalties for non-compliance

2 ☐ Civil penalties for non-compliance

98 ☐ Other, please specify *[free text]*

96 ☐ None *[free text]*

99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No

If yes, please provide more details on how you think they should be tailored to different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

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

1 ☐ The organisation
2 ☐ Named individual.
3 ☐ Both
4 ☐ Not applicable. I am responding as an individual
99 ☐ Don't know.

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

1 ☐ Same
2 ☐ Different
3 ☐ Not applicable. I am responding as an individual
99 ☐ Don't know.

Please provide any additional comments [free text]

Section 4: Proposal 3 – A ransomware incident reporting regime

- **A ransomware incident reporting regime.** That could include a threshold-based mandatory reporting requirement for suspected victims of ransomware.

Please find the relevant information on **Proposal 3: A ransomware incident reporting regime** in paragraphs 63-73 and Figure 4 in this consultation document.

Q29. To what extent do you agree, or disagree, that the Home Office should implement the following (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident reporting regime.	**Economy-wide mandatory reporting for all organisations and individuals.**	**Threshold-based mandatory reporting, for certain organisations and individuals.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Mandatory reporting for all organisations excluding individuals.** . *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based mandatory reporting, for certain organisations excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Strongly agree					
2 Tend to agree					
3 Neither agree nor disagree					
4 Tend to disagree					
5 Strongly disagree					
99 Don't know					

Please provide any further explanation for your responses *[free text]* (optional):

Q30. How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK? (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident reporting regime.	**Economy-wide mandatory reporting for all organisations and individuals.**	**Threshold-based mandatory reporting, for certain organisations and individuals.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Mandatory reporting for all organisations excluding individuals.** *This would exclude individuals from the regime but apply it to all organisations.*	**Threshold-based mandatory reporti for certain organisations excluding individu** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Effective					
2 Somewhat effective					
3 Neither effective nor ineffective					
4 Somewhat ineffective					
5 Ineffective					
99 Don't know					

Q31. How effective do you think the following would be in increasing the Government's ability to tackle and respond to the ransomware threat to the UK? (please mark your response with an X in each column):

	Continuation of the existing voluntary ransomware incident reporting regime.	**Economy-wide mandatory reporting for all organisations and individuals.**	**Threshold-based mandatory reporting, for certain organisations and individuals.** *For example, the threshold could be based on size of the organisation and/or amount of ransom demanded from the organisation or individual.*	**Mandatory reporting for all organisations and individuals.** .	**Threshold-based mandatory reporting, for certain organisations excluding individuals.** *This would exclude individuals from the regime, and set a threshold for its application to organisations, e.g. based on the size of the organisation and/or amount of ransom demanded.*
1 Effective					
2 Somewhat effective					
3 Neither effective nor ineffective					
4 Somewhat ineffective					
5 Ineffective					
99 Don't know					

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

1 ☐ Organisation's annual turnover in the UK
2 ☐ Organisation's number of employees in the UK
3 ☐ The sector organisation is operating in.
4 ☐ Amount of ransom demanded.

98 ☐ Other, please specify *[free text]* _____

99 ☐ *Don't know.*

Q33. What measures do you think would aid compliance with a mandatory reporting regime? *Please select all that apply.*

1 ☐ Additional guidance to support compliance.

2 ☐ Support to manage the response and impact following an attack.

98 ☐ Other, please specify *[free text]*

96 ☐ None *[free text]*

99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No

If yes, please provide more details on how you think they should be tailored for different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

Q35. What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime? *Please select all that apply.*

1 ☐ Criminal penalties for non-compliance

2 ☐ Civil penalties for non-compliance

98 ☐ Other, please specify *[free text]*

96 ☐ None *[free text]*

99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No

If yes, please provide more details on how you think they should be tailored for different organisations and individuals and what, if any, alternative measures you would suggest? [free text]

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

1 ☐ Yes
2 ☐ No
99 ☐ Don't know.

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

1 ☐ Yes
2 ☐ No.
99 ☐ Don't know.

If no, what time frame would you recommend and why? [free text]

Q39. Do you think that an incident reporting regime should offer any of the following services to victims when reporting? *Please select all that apply.*

1 ☐ Support from cyber experts e.g., the National Cyber Security Centre (NCSC)/law enforcement
2 ☐ Guidance documents
3 ☐ Threat intelligence on ransomware criminals and trends
4 ☐ Operational updates, e.g. activities law enforcement are undertaking.
98 ☐ Other, please specify *[free text]*

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

1 ☐ Yes
2 ☐ No
99 ☐ Don't know.

Section 5: Additional comments

Q41. Do you have any other comments on our consultation proposals?

1 ☐ Yes,
2 ☐ No
99 ☐ Don't know.

If yes, please provide any additional comments [free text]:

Section 6: Call for Evidence

Alongside the consultation, we are issuing a call for evidence to collect information and data to help support accurate estimates of the impacts of these proposals.
We invite all interested parties to provide feedback and empirical evidence on the benefits, unintended effects, consistency, and coherence of the proposals.
We will produce a full Options Assessment using the information returned to this call for evidence.

Q42. [OPTIONAL] Do you have any data or evidence to demonstrate *[Free Text]:*

- the scale of ransomware impacting the UK?
- the cost of ransomware to the economy or specific businesses when either a ransom has been paid or has not?
- the impact of a targeted ban on ransomware payments for CNI owners and operators (who are regulated/ have competent authorities), and the public sector, including local government?
- the impact of either an economy wide or threshold-based ransomware payment prevention regime?
- the impact of either an economy wide or threshold based mandatory ransomware incident reporting regime?

[OPTIONAL] Are you aware of any impact the proposals may have that we have not captured in the consultation options assessment, published alongside this document? *[Free Text]*

Section 7: About you

Please use this section to tell us about yourself.

Full name	
Job title or capacity in which you are responding to this consultation exercise (for example, member of the public)	
Company name/organisation (if applicable)	
Contact details. 1) Email address OR 2) Main address including postcode	
If you would like to remain anonymous, please tick this box ☐	

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals

Any enquiries regarding this publication should be sent to us at ransomwareconsultation@homeoffice.gov.uk.