April 8, 2025

The Home Office
2 Marsham Street
London, SW1P 4DF
United Kingdom

By email: ransomwareconsultation@homeoffice.gov.uk

Responses also submitted via homeofficesurveys.homeoffice.gov.uk

Re: Ransomware Legislative Proposals: Government Consultation

The Institute of International Finance (IIF) welcomes the opportunity to respond to the UK Home Office's consultation on proposed legislative measures to combat ransomware. The answers to the specific consultation questions are set out in the Annex of this letter and have been submitted via the survey tool.

The IIF represents approximately 400 globally active financial institutions from over 60 geographies, drawn from the banking, insurance, securities, asset management, payments and other sectors. Many of our members are particularly interested in the cross-border implications of cybersecurity requirements, including ransomware prevention and response frameworks.

While we appreciate the UK Home Office's comprehensive consideration of ransomware threats and proposed legislative response, we believe several aspects of the proposal warrant reconsideration to avoid unintended consequences and to ensure effectiveness in combating ransomware.

We fully support the UK government's objective to reduce the flow of money to ransomware criminals and to improve the reporting of ransomware incidents. However, we are concerned that certain elements of the proposals, particularly the ban on ransomware payments for critical national infrastructure (CNI) operators, could potentially create significant challenges for financial institutions and their customers. It should be noted that ransomware payments are typically a last resort option, with organizations generally exploring all other avenues before considering making a ransomware payment. The decision to pay often follows careful risk assessment when no viable alternatives exist to recover critical systems or protect sensitive data.

Background

Based on our members' experience with ransomware incidents and related regulatory frameworks globally, we have identified several high-level themes that we reflect in our individual survey responses:

- **Definition and Scope**: There appears to be a lack of clarity regarding which entities would be considered CNI operators. The financial services sector is extensively regulated, with significantly more entities in scope of designation as a CNI operator than may have been anticipated by the consultation. We believe greater clarity is needed on the scope of coverage to properly assess the impact.

- **Supply Chain Implications**: The potential extension of the ban on ransomware payments to organizations across the supply chains of CNI operators could exponentially expand the scope of the ban and may create significant challenges for financial institutions that could face unintended disruptions to their operations and services. A blanket ban could impact financial institutions' ability to maintain critical services for customers, counterparties, and consumers,

particularly when attacks target interconnected systems or third-party service providers essential to financial operations.

- **Unintended Consequences**:

    - Regulatory circumvention: Rather than reducing ransomware attacks, a strict payment prevention regime or outright ban may drive criminal activity further underground as desperate victims seek unregulated payment alternatives outside of regulated financial channels. This would bypass the important role of financial institutions, and their critical compliance functions—including sanctions screening, transaction monitoring, and suspicious activity reporting—potentially creating greater opacity in tracking criminal activities. The result could paradoxically be reduced visibility and cooperation with authorities, as organizations may be disincentivized to report attacks or may handle them through unregulated channels.

    - Disproportionate Impact on SMEs: The current proposal could leave small and medium-sized enterprises (SMEs) particularly vulnerable. A ransomware attack that might be manageable for a large financial institution could be catastrophic for a smaller company, potentially leading to business failure. The Home Office should consider the disproportionate impact an outright ban may have on smaller businesses.

    - Escalation of Attack Severity: A rigid ban on ransomware payments could lead threat actors to employ more extreme tactics to force organizations to pay. If attackers know payments are prohibited, they may target more critical services or increase the severity of their attacks to create sufficient pressure that overwhelms the deterrent effect of the ban. This could potentially lead to greater harm to customers, counterparties, and the broader public than would have occurred if a more flexible approach were permitted.

- **Distinguishing National Security from Financial Stability**: The Home Office runs the risk of conflating national security with financial stability in its ransomware proposal, despite these domains requiring fundamentally different policy approaches. The UK Department for Science, Innovation and Technology's (DSIT) April 2025 Cyber Security and Resilience Policy Statement (CP 1299)[1] illustrates this issue through its proposed "powers of direction," which would grant the Secretary of State authority to direct both regulated entities and regulators based solely on "national security" grounds. While national security imperatives are valid, CP 1299 fails to acknowledge that financial stability operates under distinct mandates with different governance frameworks and timeframes. Financial stability requires maintaining market confidence, ensuring continuous operation of payment systems, and preserving critical financial services—all regulated under specific impact tolerances (24 hours for payment systems under the UK's Operational Resilience framework). The Home Office proposal similarly lacks this nuance, failing to address how firms would meet service restoration deadlines while complying with a payment ban. In certain scenarios, the inability to make a ransomware payment or the requirement to seek pre-approval could trigger cascading failures across payment and settlement services with systemic implications for financial stability and market confidence. We therefore advocate for a flexible approach that explicitly recognizes the distinct nature of financial stability risks and preserves appropriate regulatory authority for financial regulators when addressing cybersecurity threats to the financial system.

- **Cross-Border Complexity**: Many financial institutions operate across multiple jurisdictions with varying legal frameworks regarding ransomware payments. A UK-specific ban could create significant compliance challenges for global institutions that must navigate potentially conflicting regulatory requirements. Consideration should be given to how the ban would apply to multinational organizations or to payments under their cyber insurance policies if payment is legal in some jurisdictions but not others.

- **UK Competitiveness Considerations**: The UK would be implementing a stricter approach than other major financial centers, potentially placing UK firms at a competitive disadvantage at a time when the UK is seeking to enhance its attractiveness as a global financial hub and support economic growth. This concern is particularly relevant given HM Treasury's recently published Statement of Strategic Priorities to the National Wealth Fund,[1] which explicitly identifies growth as the government's top priority. The economic implications of the ransomware proposal should be carefully evaluated against the UK's strategic business priorities.

- **Insurance Market Impacts**: A ban could invalidate some existing cyber insurance policies and would likely require a reassessment of the UK cyber insurance market. Many insurers play a crucial role in both pre-incident prevention and post-incident response, providing essential technical expertise and support that goes beyond payment facilitation. The proposal could necessitate significant revisions to post-incident response mechanisms and protocols. The Home Office should further consider and seek stakeholder input on how a ban would affect existing policies and coverage structures before taking final action.

- **Confidentiality and Privacy Concerns**: The evolution of ransomware attacks presents additional confidentiality and privacy challenges, with recent attacks increasingly focused on data exfiltration and publication of sensitive customer data, rather than system encryption. A rigid payment ban could prevent financial entities from making payments to protect customers' privacy and potentially expose them to fraud and privacy violations. Further, any data collected through mandatory reporting regimes must be protected with strong confidentiality provisions, including exemption from freedom of information requests, to encourage full cooperation and protect sensitive data. This is particularly critical when data exfiltration has occurred, as the public disclosure of reported information could further harm customers whose data has been compromised.

- **Limitations of Payment Bans**: Evidence suggests that regulatory approaches focused solely on payment bans may be ineffective; ransomware payment bans implemented in some jurisdictions have not demonstrated a measurable reduction in attack frequency. The Institute for Security and Technology's Ransomware Task Force notes in its report, "Roadmap to Potential Prohibition of Ransomware Payments" that in cases where ransomware payment bans have been introduced among government organizations, there has not been a clear decrease in ransomware attacks against these entities. [2]

- **Practicality of Payment Prevention Regime**: The proposed payment prevention regime would likely create significant bottlenecks during time-critical incidents. When organizations are facing ransomware attacks, the ability to respond quickly is crucial. A pre-approval process would force victims to navigate bureaucratic requirements precisely when they are most vulnerable and when every minute of system downtime creates additional business impact.

- **Alignment of Reporting Timelines**: Financial institutions and other highly regulated organizations already operate under multiple reporting regimes with varying timelines which can have significant operational implications, particularly during crisis situations. Cross-border supervisory colleges may create additional operational challenges with cascading reporting requirements - precisely the issue supervisory colleges aim to streamline through coordination. The proposed 72-hour reporting timeline for ransomware incidents must carefully consider the existing reporting landscape. Material incidents are already promptly reported to appropriate financial authorities—from the EU's Digital Operational Resilience Act's 4-hour reporting

---

[1] HM Treasury, "Statement of Strategic Priorities to the National Wealth Fund," (London: HM Government, 2024), https://www.gov.uk/government/publications/statement-of-strategic-priorities-to-the-national-wealth-fund/statement-of-strategic-priorities-to-the-national-wealth-fund-html.
[2] Institute for Security and Technology, "Roadmap to Potential Prohibition of Ransomware Payments," (April 2024), https://securityandtechnology.org/wp-content/uploads/2024/04/Roadmap-to-Potential-Prohibition-of-Ransomware-Payments.pdf.

requirement to the UK's CP17/24 proposal of 24-hour reporting windows. Notably, the UK has committed to avoiding the creation of any new additional reporting requirements, seeking instead to leverage and consolidate existing reporting mechanisms. Further, the recent DSIT Policy Statement (CP1299) acknowledges the need for coordination between regulatory frameworks. [3] We strongly encourage this coordination to extend to incident reporting timelines, which should be harmonized across frameworks to prevent duplicative requirements that could impede critical incident response.

Alternative Approaches

Rather than focusing primarily on payment restrictions or pre-approval frameworks, the IIF and its members suggest the following recommendations:

- **Uplifting Cybersecurity Capabilities**: Recent research suggests that allowing organizations the flexibility to pay ransoms under certain conditions may actually serve to strengthen incentives to invest in cybersecurity.[4] Iwasaki (2025) finds that organizations see greater value in their security investments when they maintain the option to restore operations through ransom payment, compared to scenarios where such payments are prohibited, severely limiting business continuity options. Instead of implementing payment bans and/or restrictions that can inadvertently penalize victims, efforts should concentrate on strengthening baseline cybersecurity capabilities, improving threat intelligence sharing, and developing more effective coordinated law enforcement responses. Resources would be better allocated toward elevating security standards across all sectors, with particular emphasis on supporting vulnerable organizations.

- **Emphasis on Supportive Compliance Framework**: Instead of penalties for non-compliance, we recommend implementing a supportive compliance framework featuring clear definitions and scope of application, secure communication channels with authorities, technical recovery assistance, collaborative threat intelligence sharing forums, and transitional periods to accommodate the need to adapt existing protocols.

- **Consideration of Existing Frameworks**: Financial institutions already operate under comprehensive regulatory frameworks that require sophisticated risk management, cybersecurity controls, and incident reporting. These arrangements have largely served the industry well in preventing and responding to ransomware attacks.

- **Targeted Sanctions Approach**: The Home Office should consider implementing restrictions tied specifically to sanctioned entities rather than broad payment bans. This approach would allow for more precise targeting of criminal organizations. Further, a sanctions-based approach can integrate with existing global sanctions frameworks, facilitating international coordination and reducing compliance complexity for multinational organizations.

- **Streamlined Reporting**: While existing ransomware reporting frameworks typically focus on incidents with a material impact on critical services, it appears the Home Office proposal is intended to capture all ransomware incidents regardless of materiality. We recommend a tiered approach that allows for baseline reporting at the outset of an incident, with more comprehensive reporting as a clearer picture of the incident emerges. In general, material incidents affecting critical services are promptly reported to appropriate financial authorities under existing reporting frameworks. We encourage the Home Office to access existing information through information sharing rather than establish parallel reporting channels that would unnecessarily complicate incident response during critical periods. For less material

[3] Ibid DSIT.
[4] Masaki Iwasaki, "Economic Analysis of Ransomware Payment Prohibitions," International Cybersecurity Law Review (2025), https://link.springer.com/article/10.1365/s43439-025-00137-5.

incidents that would not trigger existing reporting obligations but would still provide valuable intelligence, an ex post reporting mechanism could serve the Home Office's objective of understanding the broader ransomware landscape while allowing affected firms to engage in mitigation and recovery activities during active incidents.

- **Information Sharing**: Mandatory reporting regimes are most effective when they focus on collaboration rather than punishment, ensuring victims feel comfortable sharing detailed information without fear of penalties. We would emphasize the importance of enhancing collaborative information sharing between industry and government without punitive frameworks for victims, incorporating robust anonymization techniques and secure data handling practices to maintain absolute confidentiality of shared intelligence. All submitted data should be subject to strict confidentiality safeguards and limited access protocols.

- **International Harmonization**: We strongly encourage the UK government to work toward international harmonization of ransomware response frameworks. The cross-border nature of both financial services and cybersecurity threats necessitates coordinated global approaches rather than jurisdiction-specific restrictions that may create challenges for cross-border efforts to stem the flow of ransomware attacks.

- **Flexibility for Extreme Scenarios**: Should the Home Office proceed with the implementation of Proposal 1 as currently drafted, exemptions should be allowed for in cases where a ransomware payment may be necessary to prevent significant harm to financial stability or critical services. Flexibility should be permitted to allow firms to comply with their existing regulatory obligations. A clear, expedited process for obtaining exemptions should be established, with clear guidance on the threshold of service disruption the Home Office would consider tolerable before allowing a payment to restore critical services.

- **Sector-Specific Risk Assessments**: The impact of ransomware varies significantly across different sectors of the economy. We recommend developing sector-specific risk assessments and appropriate mitigation strategies rather than applying one-size-fits-all prohibitions.

Further Engagement

We encourage the UK Home Office to engage in additional discussions with industry experts before finalizing this legislative proposal. We believe that more time may be needed to carefully consider the complex implications these proposals will have on the financial sector as well as other critical sectors of the economy.

The IIF and its members look forward to engaging in additional discussions on these topics, or to clarify any aspect of our submission. We would be happy to provide further data on ransomware impacts and effective response strategies based on our members' global experience.

We thank you again for the opportunity to contribute to this important consultation.

Sincerely,

Martin Boer
Senior Director, Regulatory Affairs

Melanie Idler
Associate Policy Advisor, Regulatory Affairs

IIF Responses to Survey Questions

Ransomware Legislative Proposals: Government Consultation

Q. #	Question Text	Submission Text
10.	To what extent do you agree, or disagree, that His Majesty's Government (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?	• Strongly agree • Tend to agree • Neither agree nor disagree • Tend to disagree • **Strongly disagree** • Don't know
	Please provide any further explanation for your response (optional):	Financial institutions would face unique challenges in the event of a ransomware payment ban. As providers of essential financial services, disruptions caused by ransomware attacks could have far-reaching implications well beyond the affected institution. A ban that prevents affected organizations from making ransomware payments as a last resort option could potentially prolong service outages, impacting not only direct customers but potentially creating cascading effects through the financial system. In certain scenarios, the inability to resolve a ransomware attack expeditiously through payment could significantly impact critical financial services with potential implications for financial stability. The evolution of ransomware attacks presents additional confidentiality and privacy challenges, with recent attacks increasingly focused on data exfiltration and publication of sensitive customer data, rather than system encryption. A rigid payment ban could prevent financial entities from making payments to protect customers' privacy and potentially expose them to fraud and privacy violations. Many financial institutions operate across multiple jurisdictions with varying legal frameworks regarding ransomware payments. A UK-specific ban would create significant compliance challenges for global institutions that must navigate potentially conflicting regulatory requirements. Consideration should be given to how such a ban would apply to multinational organizations or cross-border insurance policies where ransom payments may be legal in some jurisdictions but not in the UK. Conversely, SMEs could be made particularly vulnerable by the current proposal. A ransomware attack that might be manageable for a large financial institution could be catastrophic for a smaller company, potentially leading to business failure. Any such ban should consider the disproportionate impact on smaller businesses in the financial sector. A ransomware payment ban for CNI operators could result in unintended consequences. Rather than deterring attacks, a strict payment prevention regime or outright ban may drive criminal activity further underground as desperate victims seek unregulated payment alternatives. When faced with existential threats to operations or data, victims of ransomware attacks may resort to offshore cryptocurrency exchanges, privacy-enhanced digital currencies, third-party intermediaries, or complex corporate structures to circumvent restrictions. This circumvention would bypass the important role of financial institutions, and their critical compliance functions—including sanctions screening, transaction monitoring, and suspicious activity reporting—potentially reducing visibility into criminal financial flows rather than curtailing them. Further, rigid payment bans may lead threat actors to escalate their tactics, potentially targeting more critical systems or increasing attack severity to force payment. This could result in more destructive attacks specifically designed to create sufficient operational disruption that the pressure to restore services overwhelms the deterrent effect of the ban. If a ban were to be implemented, we strongly advocate for the consideration of exceptions in cases where systemic risk or market-wide impact may result from prolonged system unavailability. However, we strongly urge the consideration of alternative approaches, such as implementing a supportive compliance framework focused on technical recovery assistance and collaboration with authorities, and threat intelligence sharing. Other approaches could include a safe harbor provision that would permit ransom payments under certain conditions. For example, companies that invest in specified levels of cybersecurity—such as robust backups, employee training, and regular penetration testing—and promptly notify authorities when an attack occurs, could be permitted to pay a ransom without incurring penalties. This approach preserves incentives to invest in preventive and reporting measures while providing a last-resort option in critical situations.
11.	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?	• Effective • Somewhat effective • Neither effective nor ineffective

Q. #	Question Text	Submission Text
		• Somewhat ineffective • **Ineffective** • Don't know
12.	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?	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
13.	What measures do you think would aid compliance with the proposed ban? Select all that apply.	• **Additional guidance to support compliance with the proposed ban** • **Tailored support to manage the response and impact following an attack** • None • Don't know • **Other (please specify):** The current proposal lacks sufficient clarity regarding which entities would be classified as CNI operators. The financial services sector is extensively regulated with significantly more entities in scope of designation as CNI operators than may have been anticipated by the consultation. Without precise definitions, the impact of the ban cannot be properly assessed or prepared for by potentially affected institutions.
14.	What measures do you think are appropriate for non-compliance with the proposed ban? *Select all that apply*.	• Criminal penalties for non-compliance • Civil penalties for non-compliance • None • Don't know • **Other (please specify):** Organizations subject to ransomware attacks are already victims of criminal activity. Imposing additional penalties would effectively punish these organizations twice – first by the criminal attackers and then by regulatory authorities. Instead of penalties, we recommend implementing a supportive compliance framework featuring clear scope definitions, secure communication channels with authorities, technical recovery assistance, expedited exemption processes for critical situations in the event a ban is implemented, collaborative threat intelligence sharing forums, and transition support for adapting existing protocols. This approach would encourage transparent reporting while ensuring organizations can make security decisions based on operational necessity rather than fear of punishment, particularly in scenarios where payment might be the only viable option to restore critical services.
15.	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?	• **Yes** • No • Don't know • Not applicable
15a.	As you responded yes to the previous question, what support would you need? (optional)	• Provide clear definitions of CNI operators. • Develop detailed implementation roadmaps and technical recovery assistance frameworks to help institutions respond to incidents without ransom payments. • Establish expedited exemption processes for situations threatening financial stability, along with cross-border guidance for multinational institutions. • Support transition from existing cyber insurance arrangements and create coordination mechanisms to align the ban with operational resilience requirements. • Establish sector-specific forums for sharing threats and recovery strategies, and provide guidance on regulatory alignment across jurisdictions.
16.	Should organisations within CNI and public sector supply chains be included in the proposed ban?	• Yes • **No** • Don't know

Q. #	Question Text	Submission Text
16a.	As you answered 'Yes' or 'No' to the previous question, please provide further explanation for your response (optional)	Extending the ban to supply chains would exponentially expand its scope beyond what may be reasonably intended or manageable. Modern CNI and public sector operations rely on complex, interconnected networks of suppliers - from major technology providers to specialized service vendors and small-scale contractors. Without clear boundaries, the ban could create significant uncertainty while potentially capturing thousands of organizations far removed from core CNI operations.
17.	Do you think there should be any exceptions to the proposed ban?	• **Yes** • No • Don't know
17a.	As you responded 'Yes' to the previous question, please provide further explanation for your response (optional)	Should the Home Office proceed with the implementation of Proposal 1 as currently drafted, exemptions should be allowed for in cases where a ransomware payment may be necessary to prevent significant harm to financial stability or critical services. Flexibility should be permitted to allow firms to comply with their existing regulatory obligations. A clear, expedited process for obtaining exemptions should be established, with clear guidance on the threshold of service disruption the Home Office would consider tolerable before allowing a payment to restore critical services.
18.	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)?	• Yes widen the ban • Yes impose a complete ban economy-wide • **No** • Don't know
19.	To what extent do you agree, or disagree, that the Home Office should implement the following:	
	1. **Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.**	• Strongly agree • Tend to agree • Neither agree nor disagree • Tend to disagree • **Strongly disagree** • Don't know
	2. **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.*	• Strongly agree • Tend to agree • Neither agree nor disagree • Tend to disagree • **Strongly disagree** • Don't know
	3. **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.*	• Strongly agree • Tend to agree • Neither agree nor disagree • Tend to disagree • **Strongly disagree** • Don't know
	4. **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.*	• Strongly agree • Tend to agree • Neither agree nor disagree • Tend to disagree • **Strongly disagree** • Don't know

Q. #	Question Text	Submission Text
	Please provide any further explanation for your response (optional):	For Question 19, we strongly disagree with the payment prevention regime described in Proposal 2. The payment prevention regime (Proposal 2), while well-intentioned, would likely create significant bottlenecks during time-critical incidents. When organizations are facing ransomware attacks, the ability to respond quickly is crucial. A pre-approval process would force victims to navigate bureaucratic requirements precisely when they are most vulnerable and when every minute of system downtime creates additional business impacts. The Home Office has not clearly explained how it would resource such a regime to provide timely assessments. There are serious concerns about whether authorities would be able to process requests quickly enough to prevent catastrophic business disruption, especially during widespread attack scenarios when multiple organizations might require simultaneous review. This prevention regime would essentially delay recovery actions while providing limited preventative benefit. Organizations would be required to engage with the Home Office, receive guidance, and discuss non-payment options, only to potentially reach the same conclusion about payment - but with weeks of additional business disruption and customer impact in the meantime. Financial institutions already maintain robust compliance frameworks to prevent payments to sanctioned entities. The additional layer of approval would duplicate existing controls without necessarily providing additional security benefits. Furthermore, the proposal creates direct conflicts with existing operational resilience requirements that mandate service restoration within specific timeframes - as little as 24 hours for critical payment systems under the UK's Operational Resilience Framework. Organizations would be placed in a very difficult position of trying to comply with contradictory regulatory obligations. For these reasons, we believe Proposal 2 would be ineffective in reducing ransomware payments while potentially increasing harm to businesses, customers, and the broader economy through extended recovery timelines.
20.	How effective do you think the following will be in reducing ransomware payments?	
	1. **Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.**	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	2. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	3. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know

Q. #	Question Text	Submission Text
	4. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
21.	How effective do you think the following will be in increasing the ability of law enforcement agencies to intervene and investigate ransomware actors?	
	1. **Economy-wide payment prevention regime for all organisations and individuals not covered by the ban set out in Proposal 1.**	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	2. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	3. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	4. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
22.	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.*	• Organisation's annual turnover in the UK • Organisation's number of employees in the UK • The sector the organisation is operating in • Amount of ransom demanded • Don't know • Other (please specify): [Intentionally left blank]
23.	What measures do you think would aid compliance with a payment prevention regime? *Please select all that apply.*	• **Additional guidance to support compliance** • **Support to manage the response and impact following an attack** • None • Don't know • **Other** (please specify):

Q. #	Question Text	Submission Text
		Clear definition of scope and applicability is essential for any payment prevention regime, with organizations needing precise understanding of which entities are covered, especially in complex corporate structures and supply chains. The regime should also include secure communication channels for confidential consultation with authorities during incidents, detailed technical assistance focused on recovery without payment, expedited exception processes for critical situations where restrictions could cause disproportionate harm, regular industry-specific forums to share evolving threat intelligence, and transition support for organizations to adapt existing cyber insurance and incident response protocols. These combined measures would provide organizations with the practical tools and clarity needed to navigate compliance requirements while effectively managing cybersecurity risks.
24.	Do you think these compliance measures need to be tailored to different organisations and individuals?	• **Yes** • No
25.	What measures do you think are appropriate for managing non-compliance with a payment prevention regime? Please select all that apply.	• Criminal penalties for non-compliance • Civil penalties for non-compliance • None • Don't know • **Other** (please specify): Organizations affected by ransomware attacks are already victims of criminal activity. Imposing additional penalties—whether criminal or civil—would effectively create a double victimization scenario: first by the attackers and then by regulatory authorities. The regulatory focus should be on strengthening organizational resilience and coordinated response rather than punishing victims who may have exhausted all other technical and operational options before considering payment.
26.	Do you think these non-compliance measures need to be tailored to different organisations and individuals?	• **Yes** • No
26a.	As you responded 'Yes' to the previous question, 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? (optional)	Rather than focusing primarily on punitive measures, we recommend concentrating efforts on strengthening baseline cybersecurity capabilities, improving threat intelligence sharing, and developing more effective coordinated law enforcement responses. Resources would be better allocated toward elevating security standards across all sectors, with particular emphasis on supporting vulnerable organizations.
27.	For those reporting on behalf of an organisation, who do you think should be legally responsible for compliance with the regime?	• The organisation • Named individual • Both • Don't know • Not applicable. I am responding as an individual [Intentionally left blank]
28.	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?	• The organisation • Named individual • Both • Don't know • Not applicable. I am responding as an individual [Intentionally left blank]
	Please provide any additional comments (optional):	We decline to select a specific option (organization, named individual, or both) because we disagree with the premise of imposing penalties on victims of ransomware attacks. Instead of focusing on penalties for non-compliance, we recommend implementing a supportive compliance framework that emphasizes collaboration and assistance. This approach would encourage transparent reporting while ensuring organizations can make security decisions based on operational necessity rather than fear of punishment, particularly in scenarios where payment might be the only viable option to restore critical services. As previously observed, an outright ban with severe penalties could encourage organizations to hide attacks and pay ransoms surreptitiously, undermining transparency and hindering collective efforts to combat cyber threats. If the Home Office proceeds with implementing compliance measures notwithstanding these concerns, we would strongly advise against

Q. #	Question Text	Submission Text
		imposing personal liability on named individuals within an organization. The complex and time-sensitive nature of ransomware incidents makes individual attribution of responsibility inappropriate, especially when decisions are typically made collectively under significant duress and with incomplete information. Furthermore, enforcement presents considerable practical challenges, particularly regarding liability determination. The Home Office proposal doesn't distinguish between vulnerabilities caused by inadequate security practices versus those caused by end-user behavior (e.g. clicking on phishing emails), making liability assignment complex. The involvement of multiple intermediaries in the payment process, the fact that financial institutions processing payments may not be informed that a transaction relates to ransomware, and the use of offshore cryptocurrency services, also contribute to significant enforcement difficulties.
29.	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):	
	1. **Continuation of the existing voluntary ransomware incident reporting regime.**	• **Strongly agree** • Tend to agree • Neither agree nor disagree • Tend to disagree • Strongly disagree • Don't know
	2. **Economy-wide mandatory reporting for all organisations and individuals.**	• Strongly agree • **Tend to agree** • Neither agree nor disagree • Tend to disagree • Strongly disagree • Don't know
	3. **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.*	• Strongly agree • Tend to agree • **Neither agree nor disagree** • Tend to disagree • Strongly disagree • Don't know
	4. **Mandatory reporting for all organisations excluding individuals**. *This would exclude individuals from the regime, but apply it to all organisations.*	• Strongly agree • Tend to agree • Neither agree nor disagree • **Tend to disagree** • Strongly disagree • Don't know
	5. **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.*	• Strongly agree • Tend to agree • Neither agree nor disagree • **Tend to disagree** • Strongly disagree • Don't know
	Please provide any further explanation for your response (optional):	The Home Office's proposal to capture all ransomware incidents regardless of materiality departs from existing frameworks that focus on materially impactful incidents affecting critical services. We recommend a tiered approach that allows for baseline reporting initially, with more comprehensive details following as the incident picture clarifies. Material incidents affecting critical services are already promptly reported to financial authorities under existing frameworks with timelines ranging from 4 hours (under the EU's Digital Operational Resilience Act, DORA) to 24 hours (as currently proposed in the UK PRA's CP17/24). Rather than establishing parallel reporting channels that complicate incident response during critical periods, the Home Office should access this existing information through information sharing arrangements. For less material incidents that wouldn't trigger existing obligations but still provide valuable intelligence, an ex post or periodic aggregated reporting mechanism would better achieve the objective of understanding the broader ransomware landscape while allowing affected organizations to focus on mitigation and recovery activities. This approach would prevent overwhelming authorities

Q. #	Question Text	Submission Text
		with information of limited value while supporting a reporting regime focused on serious incidents rather than capturing all cyber events. Any reporting framework must include strong confidentiality protections, including Freedom of Information request exemptions, to provide victims absolute assurance that sensitive information about vulnerabilities, attack vectors, and business impacts won't create additional risk through public disclosure—especially critical in data exfiltration cases where such disclosure could further harm affected customers.
30.	How effective do you think the following would be in increasing the Government's ability to understand the ransomware threat to the UK?	
	1. **Continuation of the existing voluntary ransomware incident reporting regime.**	• **Effective** • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	2. **Economy-wide mandatory reporting for all organisations and individuals.**	• Effective • **Somewhat effective** • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	3. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	4. **Mandatory reporting for all organisations excluding individuals**. *This would exclude individuals from the regime, but apply it to all organisations.*	• Effective • **Somewhat effective** • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	5. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
31.	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?	

Q. #	Question Text	Submission Text
	1. **Continuation of the existing voluntary ransomware incident reporting regime.**	• **Effective** • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	2. **Economy-wide mandatory reporting for all organisations and individuals.**	• Effective • **Somewhat effective** • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	3. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
	4. **Mandatory reporting for all organisations excluding individuals**. *This would exclude individuals from the regime, but apply it to all organisations.*	• Effective • **Somewhat effective** • Neither effective nor ineffective • Somewhat ineffective • Ineffective • Don't know
	5. **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.*	• Effective • Somewhat effective • Neither effective nor ineffective • Somewhat ineffective • **Ineffective** • Don't know
32.	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.	• Organisation's annual turnover in the UK • Organisation's number of employees in the UK • **The sector organisation is operating in** • Amount of ransom demanded • Don't know • **Other** (please specify): The sector that an organization is operating in should be the primary determining factor for establishing reporting thresholds, rather than simple quantitative metrics like employee count or revenue. Different sectors have varying levels of systemic importance and face distinct operational constraints that simple size-based thresholds cannot adequately capture. Any threshold-based approach being considered should be evidence-based, with clear justification for why certain sectors, organizations, or metrics are included, with due consideration of the varying impact of ransomware on different sectors and their recovery capabilities. Poorly designed thresholds could inadvertently redirect attacks toward organizations falling below reporting thresholds.

Q. #	Question Text	Submission Text
		If the Home Office proceeds with a threshold-based approach, we strongly recommend extensive consultation with sectoral regulators to ensure that reporting frameworks are effective and complement rather than conflict with existing regulatory obligations.
33.	What measures do you think would aid compliance with a mandatory reporting regime? Please select all that apply.	• **Additional guidance to support compliance** • **Support to manage the response and impact following an attack** • None • Don't know • **Other** (please specify): For financial institutions specifically, there must be careful coordination between any new reporting regime and existing requirements to avoid situations where compliance with reporting obligations could impede critical service restoration efforts. Reporting requirements must be compatible with other regulatory obligations, such as operational resilience requirements that mandate service restoration within strict timeframes (e.g. 24 hours for payment systems under the UK Operational Resilience Framework).
34.	Do you think these compliance measures need to be tailored for different organisations or individuals?	• **Yes** • No
35.	What measures do you think are appropriate for managing non-compliance with a mandatory reporting regime? Please select all that apply.	• Criminal penalties for non-compliance • **Civil penalties for non-compliance** • None • Don't know • Other (please specify):
36.	Do you think these non-compliance measures need to be tailored for different organisations and individuals?	• **Yes** • No
37.	Do you think the presence of a mandatory incident reporting regime will impact business decisions of foreign companies and investors?	• **Yes** • No • Don't know
38.	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?	• **Yes** • No • Don't know

39.	Do you think that an incident reporting regime should offer any of the following services to victims when reporting? Please select all that apply.	• **Support from cyber experts e.g. the National Cyber Security Centre (NCSC)/law enforcement**
		• **Guidance documents**
		• **Threat intelligence on ransomware criminals and trends**
		• **Operational updates e.g. activities law enforcement are undertaking.**
		• **Other (please specify):**
		In addition to the support options listed, an effective incident reporting regime should offer:
		  ○ Secure communication channels with dedicated points of contact who understand the financial sector's unique operational requirements
		  ○ Real-time technical assistance from specialized cybersecurity experts who can provide customized advice, negotiation services, and other specialized resources if internal capabilities are overwhelmed
		  ○ Legal guidance on regulatory compliance obligations across multiple jurisdictions
		  ○ Assistance with coordination between different regulatory bodies to avoid duplicative reporting requirements
		  ○ Post-incident analysis that identifies patterns and provides actionable intelligence back to reporting organizations
		  ○ Anonymized case studies of similar incidents and successful resolution strategies

40.	Should mandatory reporting cover all cyber incidents (including phishing, hacking etc.), rather than just ransomware?	• Yes • **No** • Don't know

Q. #	Question Text	Submission Text
41.	Do you have any other comments on our consultation proposals?	• **Yes** • No • Don't know
	If yes, please provide any additional comment (optional):	The IIF appreciates the UK Home Office's commitment to addressing the growing ransomware threat. However, we believe several aspects of the proposal require reconsideration: • Distinguishing National Security from Financial Stability: The Home Office runs the risk of conflating national security with financial stability in its ransomware proposal, despite these domains requiring fundamentally different policy approaches. The recent Cyber Security and Resilience Policy Statement (CP 1299)[1] illustrates this issue through its proposed "powers of direction," which would grant the Secretary of State authority to direct both regulated entities and regulators based solely on "national security" grounds. While national security imperatives are valid, CP 1299 fails to acknowledge that financial stability operates under distinct mandates with different governance frameworks and timeframes. Financial stability requires maintaining market confidence, ensuring continuous operation of payment systems, and preserving critical financial services—all regulated under specific impact tolerances (24 hours for payment systems under the UK's Operational Resilience framework). The Home Office proposal similarly lacks this nuance, failing to address how firms would meet service restoration deadlines while complying with a payment ban. In certain scenarios, the inability to make a ransomware payment or the requirement to seek pre-approval could trigger cascading failures across payment and settlement services with systemic implications for financial stability and market confidence. We therefore advocate for a flexible approach that explicitly recognizes the distinct nature of financial stability risks and preserves appropriate regulatory authority for financial regulators when addressing cybersecurity threats to the financial system. • Sector-Specific Risk Assessment: The impact of ransomware varies significantly across different sectors of the economy. We recommend developing sector-specific risk assessments and appropriate mitigation strategies rather than applying one-size-fits-all prohibitions. • Supply Chain Considerations: The current proposal lacks sufficient detail on how a payment ban would apply throughout the supply chain of CNI operators. Given the interconnected nature of modern business operations, clear guidance is needed on the extent of restrictions and how they would apply to third-party service providers, subsidiaries, and business partners. • Prevention Regime Practicality: The payment prevention regime (Proposal 2) would likely create significant bottlenecks during time-critical incidents. When firms need to restore operations quickly, the requirement to seek approval would delay recovery and potentially exacerbate both customer impacts and financial losses. The Home Office should clarify how they will resource this function to provide timely assessments. • Reporting Timelines: Financial institutions already operate under multiple jurisdictional and cross-border reporting regimes with varying timelines and scope. Material incidents affecting critical services already require prompt incident notification to appropriate financial authorities, ranging from 4 to 24 hours Recognizing the operational burdens such requirements can impose, the UK has explicitly committed to avoiding the creation of any new additional reporting requirements. The Home Office should instead focus on accessing existing information channels through enhanced regulatory cooperation rather than layering on additional reporting channels that would unnecessarily complicate incident response during critical response periods. We strongly recommend consultation with financial sector regulators to reconcile potentially conflicting requirements and ensure a harmonized, coherent approach to ransomware incident reporting that maintains operational resilience while meeting regulatory objectives. • International Harmonization: We strongly encourage the UK government to work toward international harmonization of ransomware response frameworks. The cross-border nature of both financial services and cybersecurity threats necessitates coordinated global approaches rather than jurisdiction-specific restrictions that may create compliance challenges. • Targeted Sanctions Approach: Rather than implementing a blanket ban on payments, we recommend adopting an approach modeled on the international sanctions framework, which would prohibit ransomware payments only to sanctioned entities and designated threat actors. This approach allows for more precise targeting of criminal organizations while maintaining flexibility for victims facing attacks from non-sanctioned groups. Further, a sanctions-based approach can integrate with existing global sanctions frameworks, facilitating international coordination and reducing compliance complexity for multinational organizations.

Q. #	Question Text	Submission Text
		• Collaborative Information Sharing Framework: We advocate for establishing a robust information-sharing mechanism between government and industry that prioritizes collaboration over punitive measures. This framework should incorporate strong confidentiality protections, including exemptions from freedom of information requests, to encourage full disclosure of attack details. • UK Competitiveness: The UK would be implementing a stricter approach than other major financial centers, potentially placing UK firms at a competitive disadvantage at a time when the UK is seeking to enhance its attractiveness as a global financial hub and support economic growth. The economic implications of this proposal should be carefully evaluated. • Adequate Transition Time: Any implementation of payment restrictions should include adequate transition periods to allow organizations to adapt their cybersecurity posture, incident response plans, and insurance arrangements. Consideration should also be given to the treatment of existing cyber insurance policies that may cover ransomware payments. We also note that cyber insurance plays a vital role in both ransomware prevention and response. Insurers provide crucial technical expertise and support beyond simply facilitating payments. The proposal should carefully consider how restrictions would affect these arrangements and ensure that beneficial aspects of cyber insurance coverage are preserved. • Consideration of Alternative Approaches: In lieu of the current proposal, we recommend the UK consider a more balanced approach. We recommend implementing a supportive compliance framework featuring clear baseline cybersecurity requirements, technical recovery assistance, and a conditional safe harbor for ransom payments when specific criteria are met. Organizations that demonstrate strong cybersecurity practices, maintain robust backups, conduct regular employee training, and promptly notify authorities when attacks occur could be permitted to make payments without penalties in limited circumstances where critical services are at risk. Allowing organizations the option to pay ransoms in these limited circumstances may actually strengthen their incentives to invest in cybersecurity, as they would see greater value in security investments when they can maintain operations even after an attack. This approach would encourage transparent reporting while ensuring organizations can make security decisions based on operational necessity rather than fear of punishment, particularly in scenarios where payment might be the only viable option to restore critical services.
42.	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? Please provide further information below: *Are you aware of any impact the proposals may have that we have not captured in the consultation options assessment, published alongside this document?*	Recent research on ransomware policy reveals significant challenges with outright payment bans. As highlighted in Masaki Iwasaki's 2025 study in the International Cybersecurity Law Review (https://link.springer.com/article/10.1365/s43439-025-00137-5), prohibiting ransomware payments may yield unintended consequences despite the intended goal of cutting off cybercriminals' funding sources. While such bans aim to incentivize better cybersecurity practices and reduce criminal profits, they may paradoxically discourage organizations from investing optimally in security measures or drive payments underground. Chubb, a leading provider of cyber insurance, recently issued a report on ""Navigating the Cyber Claims Landscape" (https://bit.ly/4i8oYJh). The Pay to Encounter Rate is a critical metric referenced in the report, which measures the percentage of organizations that choose to pay a ransom when faced with a ransomware attack. This metric reveals how regulatory environments, organizational policies, and cultural factors influence payment decisions. Organizations typically consider economic factors, recovery capabilities, data theft risks, consumer protection concerns, threat actor capabilities, and potentially severe outcomes when deciding whether to pay. Organizations that refuse payment often cite sanctions concerns, effective backup availability, confirmation that data hasn't been exfiltrated, or principled opposition to funding criminals. However, Iwasaki's economic analysis demonstrates that even with substantial cybersecurity investments, scenarios may arise where organizations cannot promptly restore systems without paying ransom, and refusing payment could lead to severe consequences (e.g. adverse patient outcomes in hospitals or large-scale exposure of sensitive information). The Institute for Security and Technology's Ransomware Task Force recommends alternatives to blanket payment bans in its "Roadmap to Potential Prohibition of Ransomware Payments" report. A more balanced approach combining clear cybersecurity standards, broader data breach notification requirements, and conditional safe harbors for ransom payments under strict conditions would likely prove more effective than outright prohibition. This framework would preserve organizations' incentives to invest in preventive measures while providing options in critical scenarios without automatic penalties.

Q. #	Question Text	Submission Text
		Effective ransomware policy must account for both criminal and victim incentives rather than driving attacks into less regulated channels, and potentially hampering investment in security measures. Such nuanced regulatory frameworks can better protect organizations while fostering stronger cybersecurity practices across sectors.