UK Government's take on ransomware: Insights from the recent consultation

Client Alert | 14 min read | 07.24.25

Ransomware attacks have escalated in frequency and sophistication, posing a significant threat to national security and critical national infrastructure ("CNI"). Cybersecurity has emerged as a core pillar of the UK's national defence strategy, as set out in the recent **Strategic Defence Review**. The Government has recognised cyber as a crucial area for modern conflict. Ransomware attacks are a significant method of attack, as a form of cybercrime which involves malicious software encrypting data and a ransom demand for its restoration or to prevent its publication. The UK has experienced a notable rise in such incidents, including attacks on Synnovis (an NHS diagnostics service provider) and Southern Water (a water company providing water to a region of the UK), both in 2024.

In response to these mounting risks, the UK Home Office launched a consultation to explore new measures and issued their **response on 22 July 2025**, outlining steps and proposals to strengthen the country's cyber resilience.

Key proposals in the consultation and responses

The consultation, conducted from January to April 2025, outlined three main proposals. The Home Office's responses are summarised in the table below.

Proposal	Home Office response
A ban on ransomware payments for public sector bodies, and CNI owners and operators. The aim of this would be to deter attacks by making it financially unattractive for attackers to target UK entities.	Strong support was shown for a targeted ban on ransomware payments for CNI and public sector bodies, with 72% of respondents in favor. 62% supported the extension of the ban to those in the CNI and public sector supply chains. Mixed responses on exceptions to the ban, relating to situations involving critical services, national security or a threat to life.
A payment prevention regime for all potential ransomware payments from the UK. Any victim would need to report an intention to pay before proceeding so that the Government could review the proposed payments to provide guidance, to aid intelligence gathering and to potentially block payments to sanctioned or terrorism-related entities. If the payment is not blocked, the victim would choose whether to proceed.	Mixed views were found on the ransomware payment prevention regime, due to concerns like the resources and capacity of organisations and time sensitivity associated with making decisions. There was a preference for an economy-wide approach (e.g. across all organisations) over threshold-based measures (e.g. size, ransom amounts, sector risks), due to potential loopholes or attackers instead targeting organisations not covered by thresholds.
A mandatory incident reporting regime for ransomware attacks within 72 hours from the incident (in line with reporting requirements involving a personal data breach), with a more in-depth report within 28 days. This would improve the Government's understanding of threats and assist law enforcement capabilities.	A new mandatory reporting regime was favored, with 63% supporting economy-wide mandatory reporting and 75% finding 72 hours to be a reasonable timeframe to report an attack.

It's not clear at this stage to what extent these proposals will make up the UK Government's legislative reform, so this is an area to keep a close eye on.

Commentary and conclusion

The Home Office aims to improve intelligence gathering, reduce payments to ransomware criminals, and enhance international cooperation to combat ransomware threats. However, several aspects remain uncertain. The responses do not clearly define the scope of each proposal, such as whether they extend to the supply chain or apply economy-wide. It is also unclear how these measures will affect international companies, especially those that might make payments through non-UK entities. A comprehensive package of victim support and guidance from the Government or other authorities will be essential for those facing this type of cyber threat. The Government might also consider other approaches to address the consultation responses, possibly through the Cyber Security and Resilience Bill.

Organisations should prepare for potential reporting requirements and anticipate revising their cybersecurity strategies by consulting subject matter experts. Businesses may be worried about disruptions caused by

reforms, so guidance from the Government and other authorities will be crucial to help navigate any new requirements. These changes will likely impact the cyber insurance policy landscape, as some policies currently cover ransom payments.

The UK Government's recent focus on cybersecurity, particularly regarding ransomware payments, represents a significant step in the fight against cyber threats. This initiative aligns with the increased attention on cybersecurity and AI risks, as discussed in our **earlier article**. The National Cyber Security Centre ("NCSC") has highlighted the emerging digital divide due to AI-enhanced cyber threats, with similar sentiments reflected in the voluntary Codes of Practice for the **Cyber Security of AI** and **Software Security**. There is a critical shift towards cyber resilience and security, and organisations must adapt to ensure their operations remain secure and resilient against evolving cyber threats, regardless of whether they fall within the scope of any legislative reform.

Contacts

Emma Wright
Partner
London D | +44.20.7413.1315
ewright@crowell.com

Clare Sellars
Counsel
London D | +44.20.7413.1309
csellars@crowell.com

Grace Tang
Associate
London D | +44.20.7413.1353
gtang@crowell.com

