OpenVoiceNews U.K.

Transparent. Unbiased. Yours.

UK Considers Ban on Ransomware Payments by Public Sector as Cyber Threats Grow

July 29, 2025

— Categories: Defence & Security

The UK government is preparing new legislation to curb the impact of ransomware attacks, with proposals to ban certain organisations, such as NHS trusts, local councils, and critical infrastructure providers, from paying ransoms to cybercriminals. Private companies may still be allowed to make payments, but only with prior government approval,

under plans aimed at reducing the financial incentives behind such attacks.

Ransomware, malicious software that locks or steals data until a payment is made, has become a growing threat to public safety and national security. In 2024 alone, the average ransom demand exceeded $5 million, with many attacks targeting essential services. The consequences have been serious: hospitals cancelling treatments, councils losing access to core systems, and even a 158-year-old logistics firm going into administration after a single phishing email compromised its network.

Authorities say that the frequency and sophistication of ransomware attacks have increased, with international groups exploiting weak defences in both public and private systems. The rise of “Ransomware-as-a-Service” has made it easier than ever for less technically skilled criminals to launch attacks using tools sold by more experienced operators. There are also growing concerns about the use of artificial intelligence (AI) to generate deepfakes, mimic voices, and automate phishing campaigns.

Cybersecurity experts warn that these developments present a clear threat to the UK’s digital infrastructure. The National Audit Office recently found that dozens of critical government systems remain vulnerable due to outdated technology and underinvestment. These weaknesses, if left unaddressed, could be exploited not only by criminals but potentially by state-linked actors.

The proposed legislation would not only limit who can pay ransoms but also introduce a requirement for private firms to report incidents and

consult with authorities before making any payment. The aim is to bring transparency, discourage ransom payments, and help law enforcement better track and respond to threats.

While some businesses worry about the operational and financial risks of such restrictions, many cybersecurity professionals welcome the move. They argue that payments only fund further attacks and rarely guarantee full recovery of stolen or encrypted data.

Officials are urging organisations to focus on prevention, updating systems, backing up data securely, using multi-factor authentication, and rehearsing incident response plans. As ransomware becomes more sophisticated, the government's message is clear: resilience, not ransom, must be the priority.