UK National Cyber Action Plan delayed again, now aimed for December 9



The UK has again postponed its National Cyber Action Plan, now reportedly aimed for December 9. The delay follows a Lords committee warning that the country is underprepared for cascading crises.

- Officials reportedly now plan to publish the plan on December 9, after earlier aiming for mid-November.
- The plan was first due by the end of 2025 and was rebranded from a national cyber strategy to an action plan.
- A House of Lords committee said the government appears complacent about potentially catastrophic risks.
- The government will consult next year on where liability for cyber breaches should sit.

> - Sources say the key details will sit in the plan's implementation schedule.

The UK government has again delayed publication of its National Cyber Action Plan, according to people familiar with the matter cited by The Record. Officials had planned mid-November and now reportedly aim for December 9. The reasons for the latest delay are unclear, and a government spokesperson said ministers remain committed to publishing the plan.

Background

The document began as a national cyber strategy due by the end of 2025. It was later rebranded as an action plan and came close to publication in July before being postponed. The delay follows a report by the House of Lords National Resilience Committee, which warned that the government appears complacent about potentially catastrophic risks, including cyberattacks from Russia, China and Iran, and that crises could cascade across sectors.

What is known about the plan

Its contents have not been officially disclosed. The reporting understands it will have three pillars: Threat, Growth and Resilience. The NCSC chief executive has described a focus on the near space (individual organisations), the mid space (shared cloud, technology and telecom infrastructure, mostly privately held) and the far space (offensive action). Sources say the critical details will be in the implementation schedule.

Related measures include a planned consultation next year on where liability for cyber breaches should sit, a voluntary Cyber Resilience Pledge on boardroom attention and supply-chain risk, and budget funding for AI security initiatives.

Why it matters

This is a UK policy matter with no direct obligation for Saudi institutions. It is still a useful signal for firms with UK operations or suppliers, and on the direction of liability and shared-infrastructure thinking.

What to do now

1. Identify UK subsidiaries, suppliers and service providers and note any exposure to UK regulatory change.
2. Watch for the plan's publication on December 9 and review its implementation schedule once released.
3. Review third-party and supply-chain risk registers, especially for shared cloud and telecom dependencies.
4. Brief the board on the UK discussion of breach liability as context for your own accountability model.