FMBusinessDaily

UK Government cyber risk is worse than watchdog says

7 months ago

Spending watchdog the National Audit Office (NAO) is right to highlight the threat to the UK Government's cyber resilience but post-quantum security pioneers Naoris Protocol warns that it is underestimating the scale of the problem.

The NAO* says the threat is "severe and advancing quickly" and points to independent assessments of 58 Government IT systems which show "significant gaps" in cyber resilience and says the Government does not know how vulnerable at least 228 legacy IT systems are to cyber attack.

It highlights skills gaps in the UK Government and says one in three cyber security roles were vacant or filled by temporary staff in 2023/24.

However Naoris Protocol says the financial and operational damage caused by data breaches is poised to worsen dramatically, fuelled by advancements in AI, quantum computing, and the Metaverse.

New Naoris Protocol research shows nearly half of IT directors** at global enterprises predict cybercrime costs will exceed $15 trillion by 2030 – equivalent to the combined GDP of Germany, Japan, and the United Kingdom with 9% predicting it will hit $20 trillion, Naoris Protocol research shows.

Its global study** with Web3 developers shows the average cost of a data breach could climb to $5.3 million within five years, up from the current $4.88 million.

Almost all Web3 developers (97%) see the Metaverse, AI, and machine learning as accelerants for more frequent and sophisticated cyberattacks.

David Carvalho, CEO & Founder of Naoris Protocol, says: “The NAO warning is a welcome wake-up call but it should not be a surprise for the industry and the Government.

“The combination of AI and the Metaverse is creating a larger attack surface for hackers, while quantum computing threatens to undermine traditional encryption methods. The risks are real, and the cost implications are staggering.”

Naoris highlights the role that Decentralized Physical Infrastructure Networks (DePIN) can play as a solution to growing cybersecurity challenges. DePIN decentralizes critical infrastructure, such as network nodes, data centers, and cloud systems, reducing reliance on centralized entities and enhancing overall resilience.

“DePIN reduces single points of failure and empowers communities to take control of infrastructure, fostering both security and economic incentives,” Carvalho adds.

In a significant step forward, Naoris Protocol has joined the DePIN Association, solidifying its position at the forefront of decentralized cybersecurity innovation. The company’s Post-Quantum powered Decentralized Security Layer Architecture is tailored to secure systems and validate assets beyond traditional cybersecurity perimeters. By fostering trust among devices, systems, and processes, Naoris Protocol empowers industries—from finance to healthcare—to transition from isolated silos to collaborative, decentralized models.