FMBusinessDaily

Public sector pay gap is risking UK's cyber security, experts warn

1 year ago

A significant pay gap between private sector and UK government cybersecurity roles is jeopardizing national security by hindering the public sector's ability to attract and retain top talent, cyber security pioneers Naoris Protocol warn.

Its analysis shows pay for key roles in cyber security can be nearly double in the private sector compared to the public sector and warns pay has to increase to help Government combat the development of artificial intelligence, quantum computing, and Metaverse which is massively increasing cyber threats.

Data* shows mid-level roles in the private sector such as Cyber Security Analysts and Penetration Testers in London offer between £50,000 and £70,000 annually. Senior positions, including Security Managers and Cyber Security Architects, see salaries ranging from £80,000 to over £120,000.

In the public sector a recent posting** for a Cyber Security Adviser at the Ministry of Defence listed a salary of £36,530 per year. More senior roles***, such as the Head of Cyber Governance, Risk, and Compliance, are advertised with salaries starting at £67,820, the analysis by Naoris Protocol found.

The pay gap has serious consequences, the Naoris Protocol study indicates. It cites a recent report**** by Spotlight on Corruption which found the National Crime Agency is struggling to recruit and retain staff with jobs in cybercrime units being left vacant. The report blames the loss of staff on low pay and poor morale, noting that NCA employees earn less than their counterparts in both the police force and private sector.

A report***** from Government spending watchdog the National Audit Office (NAO) says independent assessments of 58 Government IT systems show "significant gaps" in cyber resilience and that the Government does not know how vulnerable at least 228 legacy IT

systems are to cyber attack. It warns that one in three cyber security roles were vacant or filled by temporary staff in 2023/24.

David Carvalho, CEO & Founder of Naoris Protocol says: “The risks to UK national security from cyber crime are real and the potential costs and damage to critical national infrastructure are staggering.

“It is vital that the Government can attract top talent for key cyber security roles and worrying that so many roles are left vacant. It is, however, not that surprising when skilled people can earn so much more in the private sector.

“The UK Government needs to address the pay gap in order to safeguard the country’s digital infrastructure and competitive pay is essential to attract and retain the skilled people needed to combat evolving cyber threats.”

Naoris highlights the role that Decentralized Physical Infrastructure Networks (DePIN) can play as a solution to growing cybersecurity challenges.

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.