FMBusinessDaily

Study reveals global enterprises scramble as AI powered cyber threats drain security budgets

7 months ago

New research highlights a stark reality: IT directors at major global firms are preparing for an unprecedented surge in cyber threats driven by AI, machine learning, and the Metaverse.

As cyber criminals deploy increasingly sophisticated attacks, organizations plan significant security budget increases over the next two years. A global study of IT leaders at companies with over $300 million annual turnover by post-quantum security pioneers Naoris Protocol, highlights the growing urgency to address emerging cybersecurity challenges.

Metaverse and AI: A Dangerous Nexus for Cyber Attacks

Over 60% of IT directors strongly agree, and 37% partially agree, that the convergence of the Metaverse and AI will significantly escalate cyber attacks. Hackers are expected to exploit AI and machine learning to create more sophisticated methods, making the Metaverse a prime target.

“The Metaverse, combined with AI-driven hacking, presents a perfect storm of vulnerabilities,” warned David Carvalho, CEO of Naoris Protocol.

Decentralisation’s Promises and Perils

The study also highlights heightened cyber risks in the Web3 space. While decentralised technologies offer opportunities, they also bring new threats. Only 35% of IT directors believe their organizations fully understand Web3-related risks, 46% rate their knowledge as “quite good,” and 19% report average or

poor comprehension. Around 12% say their organisation has an average understanding while 7% admit to a poor or very poor understanding of the cyber risks posed by Web3 This knowledge gap could expose critical systems to exploitation as organisations navigate decentralisation and blockchain complexities.

Some of the biggest hacks in 2024 included DMM Bitcoin in May ($305 million) and WazirX in July ($234.9 million), this underscores the growing need to secure mechanisms frequently exploited in hacks, such as private keys. Overall Web3 security breaches led to cryptocurrency losses exceeding $2.3 billion in 2024, a 31.6% increase compared to 2023, according to blockchain security firm Certik.

Budgets on the Rise: A Necessary Response

Cybersecurity budgets are set to grow significantly as risks rise. Over the past two years, 38% of IT directors reported dramatic budget increases, while 47% saw moderate growth and 15% say it is unchanged. Looking ahead, 97% expect further increases, with 25% predicting over 50% growth and 61% anticipating increases between 10% and 50% in the next two years.

What will happen to cyber security budgets over the next two years?

● 11% expect increases of up to 10%

● 35% foresee growth between 10% and 25%

● 26% predict a 25%-50% rise

● 15% expect jumps of 50%-75%

● 10% project budget increases of over 75%

● 7% project budget increases of over 75%

DePIN: The Future of Cost-Effective Cybersecurity

Decentralised Physical Infrastructure Networks (DePINs) are emerging as a promising solution for reducing the financial and operational impacts of cyber incidents. According to the study, 32% of IT directors believe adopting DePIN-based cybersecurity measures could significantly reduce costs, while 48% see a moderate impact.

Naoris Protocol’s collaboration with the DePIN Association highlights its dedication to advancing cybersecurity and digital trust through a decentralised, post-quantum approach, benefiting industries like finance, telecommunications, and healthcare

A Call to Action for IT Leaders

“The rapid evolution of the cyber threat landscape demands equally agile responses,” Carvalho stated. “Organisations must not only expand their cybersecurity budgets but also embrace innovative technologies like decentralised solutions to stay ahead of attackers.”

With the Metaverse expanding and AI threats evolving, Naoris Protocol’s research highlights the urgent need for organisations to adopt robust, forward-thinking cybersecurity strategies to tackle the challenges

of a rapidly changing digital era.