# Businesses confront escalating cyber threats and seek advanced solutions



As businesses grapple with an escalating wave of cyber threats, recent studies highlight the growing urgency for advanced protective measures. IT directors from leading global enterprises are voicing significant concerns over the increasing sophistication of cyber attacks, which include ransomware, phishing, and potential future risks from quantum computing. According to the research conducted by Naoris Protocol, nearly half of the IT directors surveyed anticipate that cybercrime costs could surpass $15 trillion by 2030. This staggering figure is roughly equivalent to the combined GDP of Germany, Japan, and the United Kingdom. Moreover, 9% of respondents even foresee costs reaching $20 trillion.

The two-year study encompasses IT directors across companies with a minimum annual revenue of $300 million in key regions such as the US, UK, EU, and APAC. Key findings reveal that 79% of respondents have seen an increase in malware attacks, with 75% reporting heightened phishing attacks. Additionally, approximately 68% of IT directors indicated they have encountered a rise in both ransomware and distributed denial of service (DDoS) attacks.

Recent incidents underscore the vulnerabilities plaguing critical infrastructure. For instance, T-Mobile’s 2024 breach—linked to a significant cyber attack involving over 100 major telecom networks globally—exposed millions of customers. Sarah Chen, Chief Information Security Officer at a Fortune 500 manufacturer, warned about the operational disruptions caused by minor technical gaps, which can harvest significant havoc within supply chains.

The findings further reflect the perceived effectiveness of cybersecurity measures in place at these enterprises. Only 55% of IT directors described their malware defence systems as excellent, with lower ratings reported for protection against phishing (53%), ransomware (45%), and DDoS attacks (50%). David Carvalho, CEO and Founder of Naoris Protocol, highlighted the need for improved architectures, emphasising that “traditional security walls haven’t been enough for a long time and are obviously no longer acceptable."

Against this backdrop, Decentralized Physical Infrastructure Networks (DePIN) appear to be gaining traction as a potential solution. Approximately 64% of IT directors believe that the market for DePIN could exceed $3 trillion by 2028 from its current valuation of $2.2 trillion. This technology decentralises critical internet infrastructure, distributing data control, encrypted transit storage, and enhancing resilience against attacks. Notable success stories in this space include Helium’s decentralized wireless network, showcasing the model's growth potential.

Simultaneously, consulting firm Accenture has announced a bold expansion of its generative AI-powered cybersecurity services aimed at strengthening corporate defences against evolving threats. Announced on 25 October 2024, this suite of services seeks to tackle the vulnerabilities that arise from digital transformation initiatives, which have been increasingly targeted by cyber criminals.

Karthik Ramakrishnan, Accenture’s Global Cybersecurity Lead, stressed the importance of this initiative, stating, “As cyber threats become increasingly sophisticated, organizations must enhance their resilience and embrace a proactive approach to cybersecurity.” The integration of machine learning algorithms into Accenture’s offerings stands out, enabling continuous improvement of threat detection capabilities. This allows organisations to effectively predict vulnerabilities while also automating incident response to reduce operational risks.

Accenture's suite is tailored to meet the unique challenges faced by various sectors, particularly in finance, healthcare, and critical infrastructure, where robust data protection is vital. The firm plans to collaborate with leading technology partners to further refine its generative AI capabilities, while also committing to educate and train cybersecurity professionals to adeptly leverage these advanced tools.

As both Naoris Protocol and Accenture highlight the challenges and solutions around cybersecurity, businesses are increasingly recognising the necessity to reassess their security strategies in the face of evolving cyber threats. The trend towards decentralisation and the introduction of generative AI show promise in equipping organisations to not only protect sensitive data but also enhance their operational resilience in a rapidly changing digital landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://it-online.co.za/2025/01/07/cybersecurity-threat-hits-15trn-as-attacks-surge/> - Corroborates the prediction by IT directors that cybercrime costs could surpass $15 trillion by 2030 and the increase in cyber attacks including ransomware, phishing, and potential future risks from quantum computing.
2. <https://it-online.co.za/2025/01/07/cybersecurity-threat-hits-15trn-as-attacks-surge/> - Supports the findings of the two-year study by Naoris Protocol involving IT directors across companies with a minimum annual revenue of $300 million in key regions.
3. <https://www.cybersecuritydive.com/news/cybersecurity-trends-outlook-2025/736929/> - Highlights recent incidents and vulnerabilities in critical infrastructure, such as the T-Mobile breach and telecom network attacks.
4. <https://www.cybersecuritydive.com/news/cybersecurity-trends-outlook-2025/736929/> - Discusses the operational disruptions caused by minor technical gaps and the need for improved cybersecurity measures.
5. <https://it-online.co.za/2025/01/07/cybersecurity-threat-hits-15trn-as-attacks-surge/> - Details the perceived effectiveness of cybersecurity measures in place at enterprises, including ratings for malware, phishing, ransomware, and DDoS attacks.
6. <https://it-online.co.za/2025/01/07/cybersecurity-threat-hits-15trn-as-attacks-surge/> - Mentions the potential of Decentralized Physical Infrastructure Networks (DePIN) as a solution and the market predictions for DePIN.
7. <https://www.cybersecuritydive.com/news/cybersecurity-trends-outlook-2025/736929/> - Supports the trend towards decentralization and the importance of addressing single points of failure in critical IT systems.
8. <https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2025/> - Discusses the integration of AI and generative AI in cybersecurity, aligning with Accenture’s expansion of AI-powered cybersecurity services.
9. <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/> - Provides context on the growing costs of cybercrime, including damage and destruction of data, stolen money, and other related costs.
10. <https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2025/> - Highlights the importance of identity transformation and the shift to an Identity-First strategy in enterprise security.
11. <https://www.cybersecuritydive.com/news/cybersecurity-trends-outlook-2025/736929/> - Emphasizes the regulatory environment and the increasing pressures on CISOs due to the heightened threat of malicious cyber activity.
12. <https://uktechnews.co.uk/2025/01/08/cyber-attacks-surge-global-giants-face-15-trillion-threat-by-2030/> - Please view link - unable to able to access data
13. <https://erp.today/accenture-expands-generative-ai-powered-cybersecurity-services-to-enhance-client-resilience/> - Please view link - unable to able to access data
14. <https://news.google.com/rss/articles/CBMirwFBVV95cUxQZHJUdGpEZFozdGw2cHBTbWYzZGR3TlJPV3RZWnVzald2TWJvLVNQVGpIQzFaZUJ4Q2EyYTVwVjZ3bm82QURSMm9rUElDcElXVGxpTllzUVJ1QmZQUUVITzluTUg1Z0pud2l4MWo2MUVteVQtS3RSdWJybl9VNFJjTy0wNjhqd1ZrT2wta09kcTJRT3Z5S2pEMVFPcXNxSlpkR2hxVFZFSEtnZGVyNUdn?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data