# Global Cybersecurity Outlook 2025 reveals rising threats and the role of AI



The Global Cybersecurity Outlook 2025, published by the World Economic Forum (WEF), underscores the increasingly complex and evolving threats in the cybersecurity realm. This comprehensive report sheds light on the dynamics that are shaping the current cybersecurity landscape and offers insights that are particularly relevant for businesses navigating these challenges.

Central to the findings is the recognition that geopolitical tensions, emerging technologies, supply chain interdependencies, and the growing sophistication of cybercrime contribute significantly to the complexities faced by organisations today. The WEF notes that nearly 60% of businesses report that their cybersecurity strategies are heavily influenced by geopolitical uncertainties. This has resulted in organisations reevaluating their trading policies and operational frameworks in response to an unpredictable environment.

A notable aspect of the report is the emphasis on the impact of artificial intelligence (AI) within the cybersecurity sector. The findings reveal that while 66% of organisations anticipate a significant influence from AI on their cybersecurity measures, there exists a concerning gap in readiness. Specifically, only 37% of organisations have implemented processes to assess the security risks associated with AI before its deployment. This highlights a pressing need for businesses to adopt proactive strategies and allocate resources effectively to bolster their cybersecurity frameworks as risks continue to escalate.

Additionally, the WEF's report advocates for global collaboration and increased investment in cybersecurity measures to enhance digital resilience and safeguard financial stability. As cyber threats become more sophisticated and scalable, the report calls for a transformative shift from traditional security approaches towards a resilience-focused strategy, catering to the evolving demands of the cybersecurity landscape.

In summary, the Global Cybersecurity Outlook 2025 by the World Economic Forum outlines critical factors affecting cybersecurity, highlights the transformative role of AI, and underscores the necessity for businesses to adapt their strategies proactively in the face of rising threats.

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

## Bibliography

* <https://guptadeepak.com/the-future-of-cybersecurity-global-outlook-2025-and-beyond/> - This link corroborates the WEF's Global Cybersecurity Outlook 2025, highlighting the complexities driven by geopolitical tensions, emerging technologies, and the growing sophistication of cybercrime.
* <https://guptadeepak.com/the-future-of-cybersecurity-global-outlook-2025-and-beyond/> - It supports the finding that nearly 60% of organizations report their cybersecurity strategies are influenced by geopolitical uncertainties, leading to adjustments in trading policies and operations.
* <https://guptadeepak.com/the-future-of-cybersecurity-global-outlook-2025-and-beyond/> - The article discusses the impact of AI on cybersecurity, noting that 66% of organizations expect AI to significantly impact their security, but only 37% have processes to assess AI security risks before deployment.
* <https://guptadeepak.com/the-future-of-cybersecurity-global-outlook-2025-and-beyond/> - It emphasizes the challenges posed by supply chain interdependencies, regulatory requirements, and the growing complexity of securing interconnected business ecosystems.
* <https://guptadeepak.com/the-future-of-cybersecurity-global-outlook-2025-and-beyond/> - The article highlights the increasing cyber risks, with ransomware remaining a top concern, and the widening skills gap in the cybersecurity workforce.
* <https://www.wwt.com/blog/key-cybersecurity-threats-and-opportunities-for-2025> - This link supports the notion that AI will play a transformative role in cybersecurity, with autonomous AI systems and weaponized decision-making posing significant risks.
* <https://www.wwt.com/blog/key-cybersecurity-threats-and-opportunities-for-2025> - It discusses the tightening regulatory landscape, including stricter requirements for data protection and cybersecurity, and the need for global data protection standards.
* <https://www.wwt.com/blog/key-cybersecurity-threats-and-opportunities-for-2025> - The article mentions the increasing regulatory pressure and the need for significant investments in compliance, policy creation, and new security products.
* <https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025?e=48754805> - This link corroborates the growing sophistication of cybercrime, including the use of AI for phishing, vishing, and social engineering attacks, as well as the continued threat of ransomware and multifaceted extortion.
* <https://cloud.google.com/blog/topics/threat-intelligence/cybersecurity-forecast-2025?e=48754805> - It supports the finding that geopolitical tensions, particularly from countries like Russia, China, Iran, and North Korea, will continue to influence cybersecurity strategies.
* <https://www.wwt.com/blog/key-cybersecurity-threats-and-opportunities-for-2025> - The article emphasizes the need for a transformative shift from traditional security approaches to a resilience-focused strategy to address the evolving demands of the cybersecurity landscape.
* <https://news.google.com/rss/articles/CBMinAFBVV95cUxPeDlleFRQTnRyd1FNUjVrV25aZWdvUTVPWk5hUk8zR1BBUE1qa2NZcjF3ZFBJQndJc2EwYnVCZndmQWpoLVFoM1F2YjNzbENSTjh0T1pzNHh3cERaMGNyZV9za1dkRDVCNVJQTnJ1NHJIS3ZFejFCdGxQMFZOU0xTeWlibGdibWM3ZE1STkhoZHQ2YkVOMXVlSWptLXM?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data