AXIS / Technology

Practical Guidance

AI

When AI Becomes Systemic Cyber Risk

How Anthropic's Mythos model signals a structural shift in cyber exposure

Written by Chris Jones

A New Class of Cyber Capability

Claude Mythos Preview is a frontier AI model developed by Anthropic, designed to advance capabilities in reasoning, code generation, and autonomous task execution. Based on reported deployments, access has been deliberately restricted to a small number of large enterprises, government bodies, and strategic partners, reflecting concerns that its capabilities could be misused to enable highly effective cyber operations at scale.

Unlike earlier models, Mythos can independently identify problems, generate solutions, and execute multi-step technical workflows with minimal human input. While this delivers clear productivity gains, it also introduces a new class of cyber exposure.

The same functionality that enables efficiency: automated reasoning, code generation, and system interaction, can be leveraged to identify vulnerabilities, develop exploit pathways, and execute coordinated cyber-attacks across multiple targets simultaneously, increasing both the speed and scale at which attacks can be deployed.

From Human-Limited to Machine-Scaled Threat

Historically, cyber-attacks have been constrained by human expertise, time, and coordination. Even sophisticated threat actors faced limits in how quickly vulnerabilities could be identified, exploits developed, and attacks deployed.

Models like Mythos materially change these constraints.

The ability to analyze environments, generate exploit pathways, and execute against multiple targets in parallel introduces a fundamentally different operating model. What was once manual becomes automated. What was once targeted becomes repeatable. What was once sequential becomes simultaneous.

Cyber risk is no longer bounded by human scale.

From Isolated Incidents to Scalable Threat

Cyber events have traditionally been episodic and contained. Even large-scale incidents required coordination and effort that limited their reach.

AI-enabled capability alters this dynamic.

A single vulnerability, particularly within widely used software, cloud infrastructure, or shared platforms, can be identified and exploited at scale. The same attack logic can be deployed across multiple organizations simultaneously, with minimal incremental effort.

This introduces a new reality: cyber events are no longer isolated. They are increasingly scalable, repeatable, and broadly deployable.

Why This Matters: Correlation of Loss

The most significant implication of this shift is the emergence of correlated loss.

AI-enabled attacks can propagate across shared dependencies: cloud providers, software ecosystems, network infrastructure, and third-party vendors. Where multiple organizations rely on the same underlying systems, a single exploit can trigger concurrent loss events.

For insurers, this challenges a core assumption of risk diversification.

In a Mythos-enabled scenario, losses may be simultaneous and concentrated, creating aggregation exposure at a level not previously contemplated in traditional cyber underwriting.

The Coverage Gap: Event vs. Liability

As the nature of cyber events evolves, a structural gap in insurance coverage becomes more pronounced.

Cyber policies are designed to respond to the event itself: incident response, system restoration, and business interruption. However, the financial consequences of a cyber event often extend beyond operational disruption.

Where an incident results in failure to meet contractual obligations, such as downtime, service interruption, or performance failure, liability shifts into Technology E&O. This includes breach of contract, service failure, and associated financial damages.

In an AI-driven, scalable event, these elements are triggered together. The disruption and the liability are inseparable, yet many insurance programs continue to treat them as distinct exposures.

The result is a fragmented insurance response to a unified loss scenario.

Market Response: Coverage May Tighten

As systemic exposure becomes clearer, underwriting response is already beginning to evolve.

Insurers are increasingly focused on aggregation risk, particularly where shared infrastructure and third-party dependencies exist. This is likely to result in:

- Greater scrutiny of dependency and concentration risk
- Broader application, or introduction, of systemic event exclusions
- Increased reliance on war and state-linked exclusions in large-scale events where attribution to a state actor is required, creating uncertainty and potential dispute
- Higher retentions and potential coinsurance on large-scale events
- More constrained limit deployment, particularly in higher layers

At the same time, underwriting will continue to shift toward a control-based approach, with emphasis on segmentation, resilience, and the ability to isolate and contain incidents.

What This Means Now

The emergence of models like Mythos signals a structural shift in cyber risk.

Organizations can no longer assess exposure solely at the individual entity level. Risk must be evaluated across systems, dependencies, and contractual obligations.

This raises a more immediate question:

Are existing insurance structures designed to respond across the full loss pathway, from initial system disruption through to downstream financial and contractual consequences?

Takeaway: A Developing, Not Hypothetical Risk

AI-driven cyber capability has the potential to shift cyber risk from severe to systemic.

As with prior evolutions in attack methodology, the gap between how risk manifests and how it is insured is already emerging. Coverage structures, underwriting approaches, and market capacity will continue to adapt.

The issue is not whether this shift occurs, but whether organizations are positioned with the appropriate controls and insurance structure to respond when it does.

Don't wait for an AI-driven cyber event to reveal where your coverage stops.

Contact our team today to review your Cyber, Technology E&O, and third-party dependency exposures, and stress-test whether your insurance program responds across the full loss pathway, from system disruption to downstream contractual liability.

Contact Us

Chris Jones
Account Executive,
Mining & Technology
+1 (778) 788-2853
Chris.Jones@axisinsurance.ca

Clive Bird
Senior Vice President,
Mining & Technology
+1 (604) 817-8072
Clive.Bird@axisinsurance.ca

Stacey Copeland
Vice President,
Mining & Technology
+1 (604) 619-7775
Stacey.Copeland@axisinsurance.ca

Tristan Smith
Business Development Specialist,
Mining & Technology
+1 (416) 885-0671
Tristan.Smith@axisinsurance.ca

About

Axis Insurance - Safeguarding the Exceptional. Axis Insurance is your strategic advantage; we cut through the complexity of risk management enabling you to confidently embrace the opportunities of tomorrow. Our role is to provide you with the best insurance value that combines coverage, service and price. We also provide personalized, quality service that includes professional insurance advice, ongoing policy maintenance and claims support. When any issue arises regarding your insurance coverage, we are your advocate, using our professional experience to best represent your individual interest. Follow Axis on LinkedIn, X, Facebook and Instagram. Stay up to date by signing up for our newsletter here.

axisinsurance.ca
#2000 – 1055 Dunsmuir Street, Box 49264, Vancouver, B.C. V7X 1L2
1-800-690-7475