



The New Economics of Cyber Risk

How CISOs, Insurers and Risk Managers respond to the Age of Frontier AI

James Tuplin, SVP and Head of International Cyber, Mosaic;
Jay Vinda, Global CISO and Cyber Risk Engineering Lead, Mosaic;
Sanith Wijesinghe, Chief Engineer, Public Sector, MITRE;
Chris Folk, Director, Cyber Solutions Cell, MITRE

“

The emergence of frontier AI models has triggered a debate across the cyber security and risk management communities – what happens when attackers gain access to systems capable of discovering vulnerabilities, generating exploits and reasoning through attack paths at unprecedented speeds. While this is a reasonable debate to be having, this framing has the risk of overstating what is actually changing.

This Thought Leadership Paper Series is a joint project from Mosaic Insurance and MITRE.

Introduction | The New Economics of Cyber Risk

How CISOs, Insurers, and Risk Managers Respond to the Age of Frontier Artificial Intelligence

Paper 1 | Beyond Patch Velocity

Rethinking Cybersecurity Strategy in a Post-Frontier AI World

Paper 2 | Beyond Vulnerability Counts

Reimagining Cyber Insurance Underwriting in a Post-Frontier AI World

Paper 3 | Buying Resilience

How Risk Managers Can Close the Gap Between the CISO and the Boardroom

The New Economics of Cyber Risk

How CISOs, Insurers and Risk Managers respond to the Age of Frontier AI

The emergence of frontier artificial intelligence (AI) models has triggered a debate across the cybersecurity and risk management communities. What happens when attackers gain access to systems capable of discovering vulnerabilities, generating exploits, and reasoning through attack paths at unprecedented speed? While this is a reasonable debate, the framing risks overstating what is actually changing.

Social engineering remains one of the most successful methods of compromise. Criminal marketplaces offer access, malware, infrastructure, and ransomware capabilities at low cost. Cybercriminals already had highly effective and cost-efficient attack techniques before frontier AI arrived.

In many respects, frontier AI is less about industrialization and more about democratization. The criminal marketplace industrialized itself over the past decade through specialization, division of labor, and capability sold as a service. What frontier AI adds on top of that is a lower skill barrier. Capabilities that previously required specialist expertise become available to a broader range of threat actors. The objective remains largely unchanged. Frontier AI does not fundamentally change what attackers are capable of achieving. It changes how quickly, cheaply, and efficiently they can achieve it. This distinction matters because it challenges several assumptions that underpin how organizations manage cyber risk.

Most organizations manage cyber risk through a combination of mitigation, transfer, acceptance and avoidance.

Most organizations manage cyber risk through a combination of mitigation, transfer, acceptance, and avoidance. These decisions are ultimately intended to move risk toward, and maintain it within, an organization's defined risk appetite.

Risk is not static, and cyber risk is unusual in having an adversary actively working against the defense. The challenge frontier AI poses is that the threat landscape may change at a velocity that outpaces the risk management programs built to track it.

While many stakeholders contribute to cyber risk management decisions, there are three groups that exert significant influence over their direction: the CISO, the cyber insurance market, and the enterprise risk management function. Each community views cyber risk through a different perspective, but all face the same question: How do we make effective decisions when the pace of change accelerates and uncertainty grows?

The New Economics of Cyber Risk

How CISOs, Insurers and Risk Managers respond to the Age of Frontier AI

This introduction, written by MITRE and Mosaic Insurance, opens a three-part series that explores these perspectives in greater detail:

1. **Beyond Patch Velocity: Rethinking Cybersecurity Strategy in a Post-Frontier AI World.** This paper examines why patching faster is not, by itself, a strategy for responding to frontier AI and how the CISO operating model may need to evolve.
2. **Beyond Vulnerability Counts: Reimagining Cyber Insurance Underwriting in a Post-Frontier AI World.** This paper explores how insurers may need to rethink underwriting signals, challenge assumptions and operate in an environment where the gap between what exists, what can be discovered, and what can be observed is widening more rapidly than before.
3. **Buying Resilience: How Risk Managers Can Close the Gap Between the CISO and the Boardroom.** This paper considers how enterprise risk managers can help to close the gap between the CISO and the boardroom, shifting the conversation from indemnity, risk transfer, and mitigation toward building organizational resilience.

The arrival of frontier AI accelerates the rate at which risk evolves and increases the uncertainty surrounding it. It does not invalidate the foundations of cybersecurity, cyber insurance, or enterprise risk management. The organizations best positioned for a post-frontier AI world are unlikely to be those that simply patch faster, buy more technology, or transfer more risk. They will be the organizations that can continuously understand their exposure, make decisions at the speed of risk, and strengthen resilience as the environment around them evolves.

The defining question in a post-frontier AI world is not whether frontier AI changes the cyber threat landscape or if cyber risk becomes unmanageable or uncertain. It is whether the operating models that underpin cybersecurity, cyber insurance, and enterprise risk management can adapt to the new pace of change and respond quickly enough when disruption occurs.

The New Economics of Cyber Risk

How CISOs, Insurers and Risk Managers respond to the Age of Frontier AI

About the Authors

James Tuplin, is the Head of International Cyber underwriting at Mosaic Syndicate where he is responsible for the cyber underwriting teams based in London, Cologne, and Dubai. James has 23 years of underwriting experience specializing in cyber and technology E&O insurance for the last 20 years.

Jay Vinda, is the CISO and Cyber Risk Engineering Lead at Mosaic Insurance. He bridges the gap between technical security concepts, business objectives and risk management strategies. Through his work, he aims to contribute towards establishing cyber insurance as a powerful risk management partner, proactively helping organizations to protect systems and become resilient to emerging threats.

Sanith Wijesinghe, Dr. Sanith Wijesinghe is the Chief Engineer for MITRE's public sector. Over the past 10 years he has overseen MITRE's R&D initiatives in blockchain, including development of the AADAPT cyber threat framework for digital assets. Most recently he led a NIST cybersecurity workshop panel discussion on "Systemic Threats, Vulnerabilities, Interoperability and Other Shared Challenges" for digital ledger based technologies.

Chris Folk, is a Senior Cybersecurity Leader at MITRE, with 25 years in cybersecurity, national critical infrastructure protection, including eight years leading the CVE Program through its 2016 federation redesign. His work focuses on the governance layer of cyber risk: how disclosure, coordination, and interpretation reduce exposure risks.

