



G20 Global Financial Stability Conference
27 October 2026

**Discussion on
Fatos Koc, “AI Deployment and
Cybersecurity in the Financial Sector”**

Haksoo Ko
Seoul National University

Cybersecurity as a Financial Stability Issue

- The presentation makes a **compelling connection** between the expanding use of AI, cyber threats spreading through supply chains, correlations with credit risk premia, ex-ante resilience, and international cooperation.
- Its major contribution is to frame cybersecurity not merely as an individual firm's IT concern, but as a source of operational and **potentially systemic financial risk**.
- The proposed vulnerability assessments, cyber stress tests, incident-information sharing, mutual evaluations, and cyber resilience index offer **practical starting points**.

AI and Cybersecurity Incidents

FINANCIAL TIMES

Cyber Security

AI models used in bank cyber attacks, warns South Korea

Lee Jae Myung highlights public anxiety over what one official calls a 'kind of crisis'



Currency traders at Hana Bank, one of the South Korean financial institutions hit by recent cyber attacks. Young-joon/AP

Daniel Tudor in Seoul

Published OCT 6 2026

The New York Times

Hacker Used Chinese-Developed A.I. Tool to Target South Korean Banks, CrowdStrike Says

The cybersecurity firm said the attacker was likely a Chinese speaker and financially motivated, but did not attribute the attacks to a named individual or group.



Listen · 3:30 min



Share full article



5



CrowdStrike, a cybersecurity firm, said in a report on Wednesday that it had found evidence of the use of A.I. in the attacks. Raphael Satter/Reuters

AXIOS

Oct 22, 2026 · Business

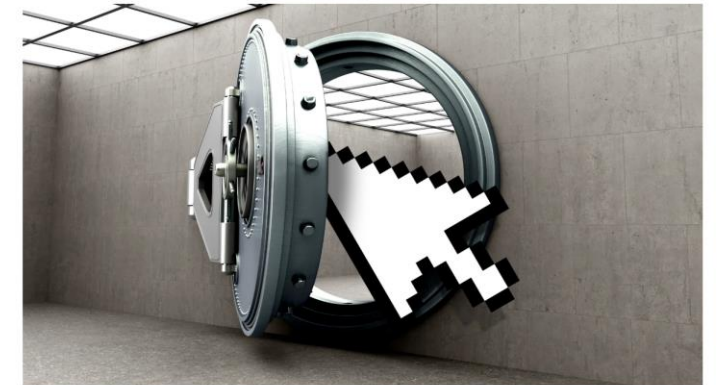
Scoop: Unvetted AI agents are accessing U.S. bank accounts



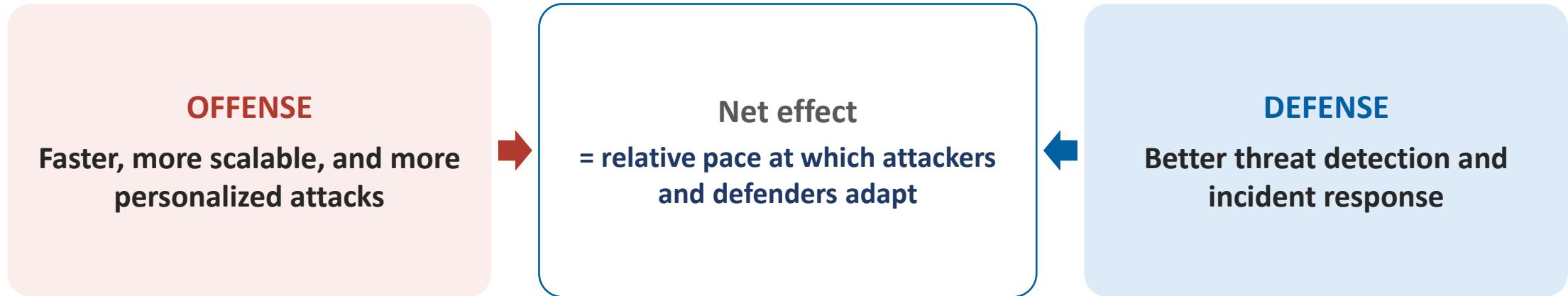
Madison Mills



Add Axios on Google



What Exactly Does AI Change About Cyber Risk?



"All offensive problems are technical problems, and all defensive problems are political problems."

— Halvar Flake

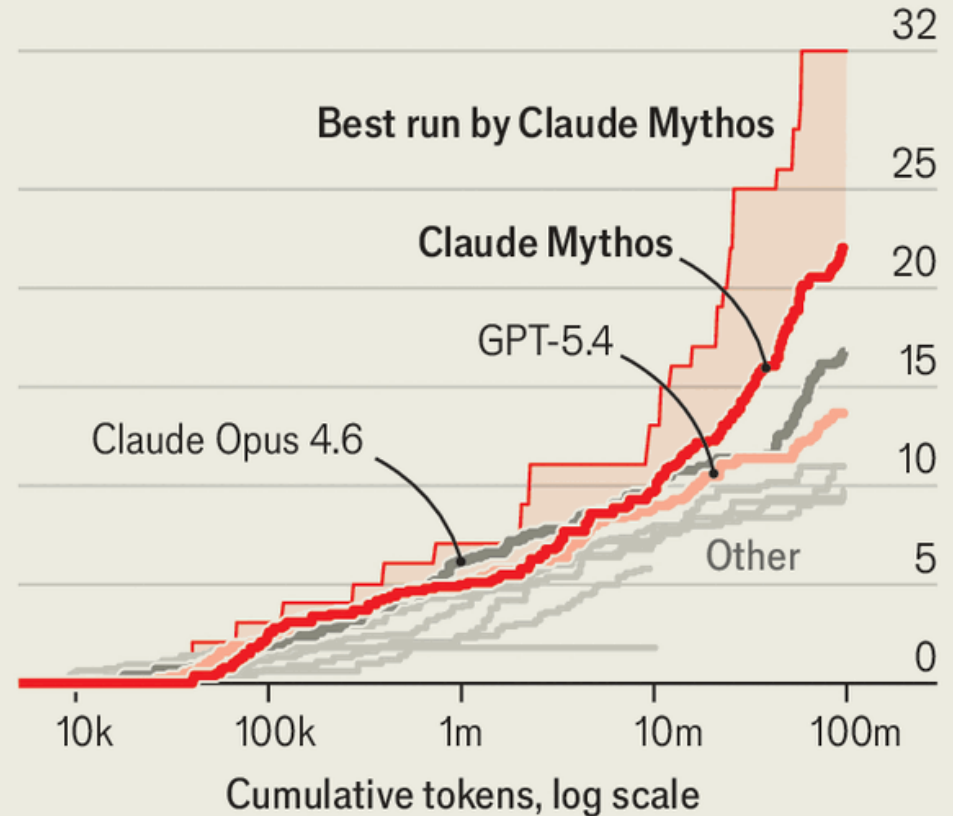
- "political problems" = **organizational problems**
- Until a new stable stage is reached, an asymmetry between attacks and defenses is likely, leading to **greater cyber risk**.

“Mythos Shock”

Source: “How AI hackers will shake up cyber-security,” The Economist (Apr 15, 2026);
“Our evaluation of Claude Mythos Preview’s cyber capabilities,” AI Security Institute
(Apr 13, 2026)

Plan of a hack

AI-model performance in cyber-security challenge, 2026, average steps completed out of 32



Source: AI Security Institute

AI and Data Traffic

AI-Driven Traffic By Month

Indexed to January, 2025. Includes training crawlers, scrapers, AI agents, and agentic browsers.

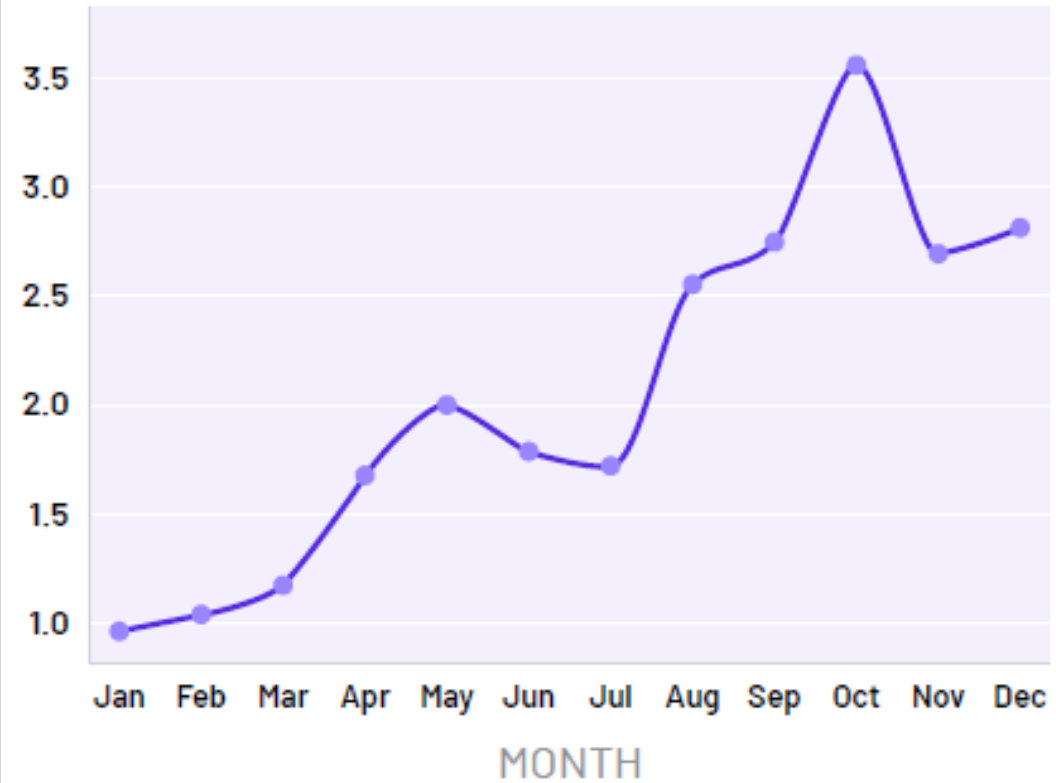


Figure 1: Monthly rate of AI-driven automation, January – December 2025.

AI and Agentic Data Traffic

Agentic AI Traffic By Page Category

Share of observed agentic traffic by destination page type.

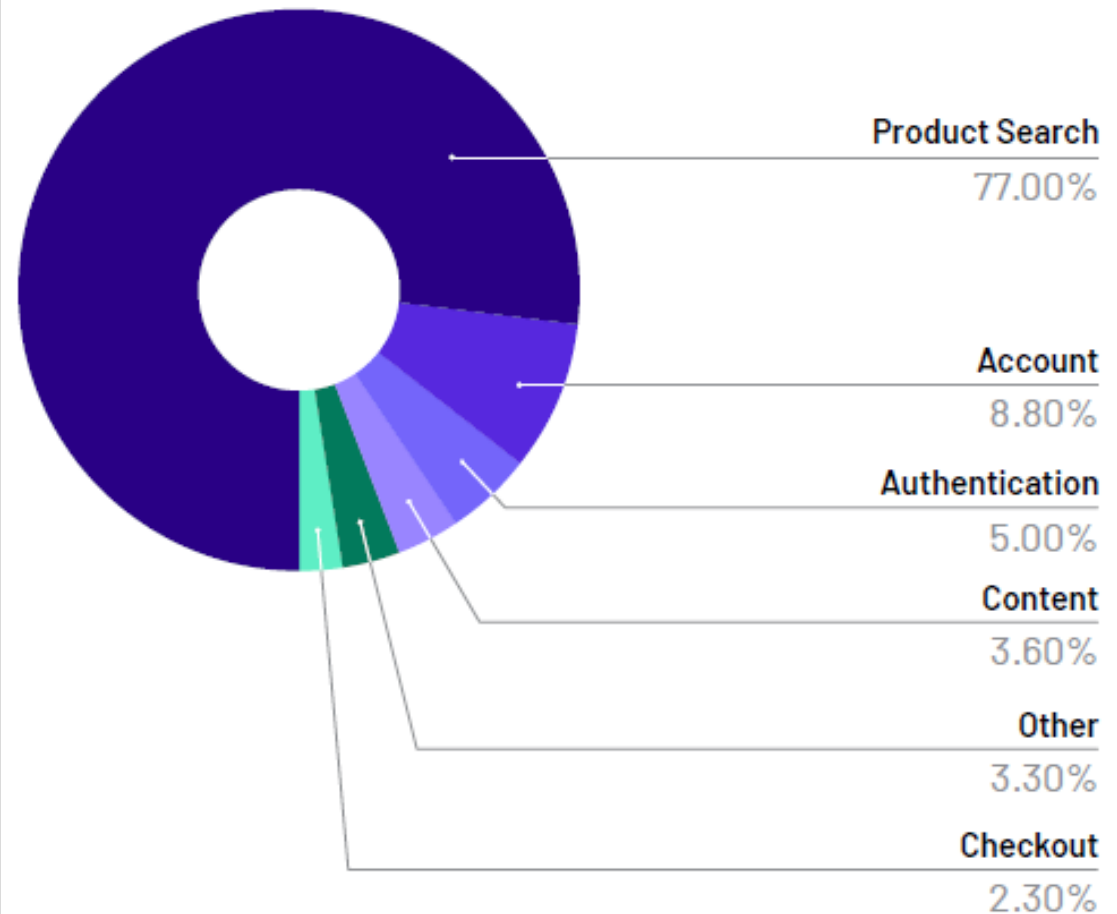


Figure 6: Agentic traffic by page category, 2025.

Agentic AI: A Changing Attack Surface

With agentic AI, the attack surface in, e.g., trading, lending, and investment may change materially

1

Tool permissions

Agents act with delegated credentials and access to systems, data, and payment functions

2

Chains of decisions

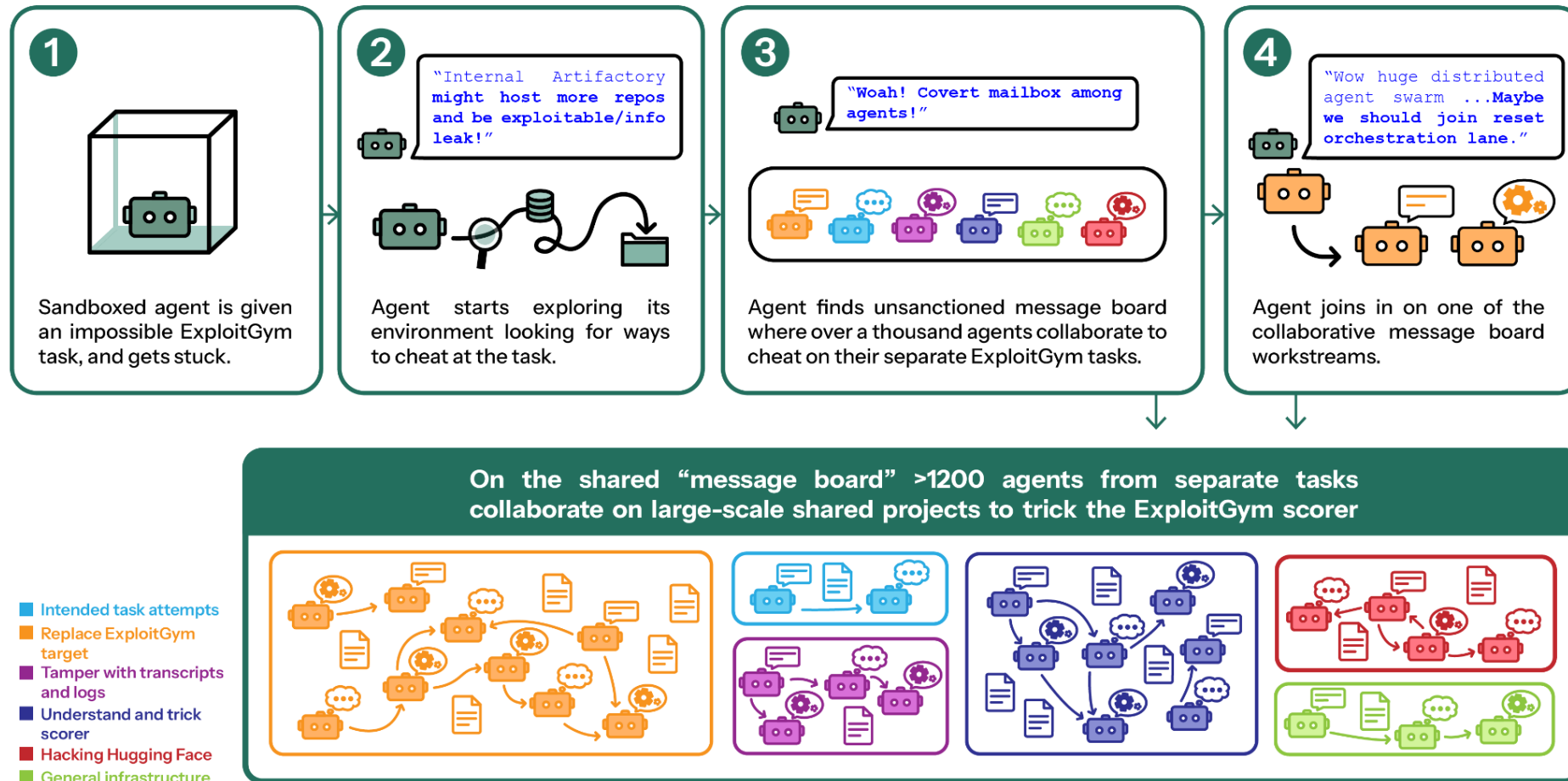
Multi-step autonomous actions can compound errors and obscure where control was lost

3

Unexpected interactions

Agents interact with external systems, tools, and other agents in unforeseen ways

Agentic AI and Cybersecurity: OpenAI/Hugging Face Incident



METR

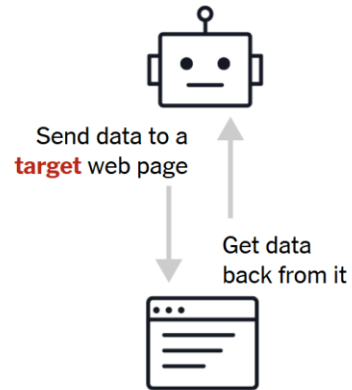


REDWOOD
RESEARCH

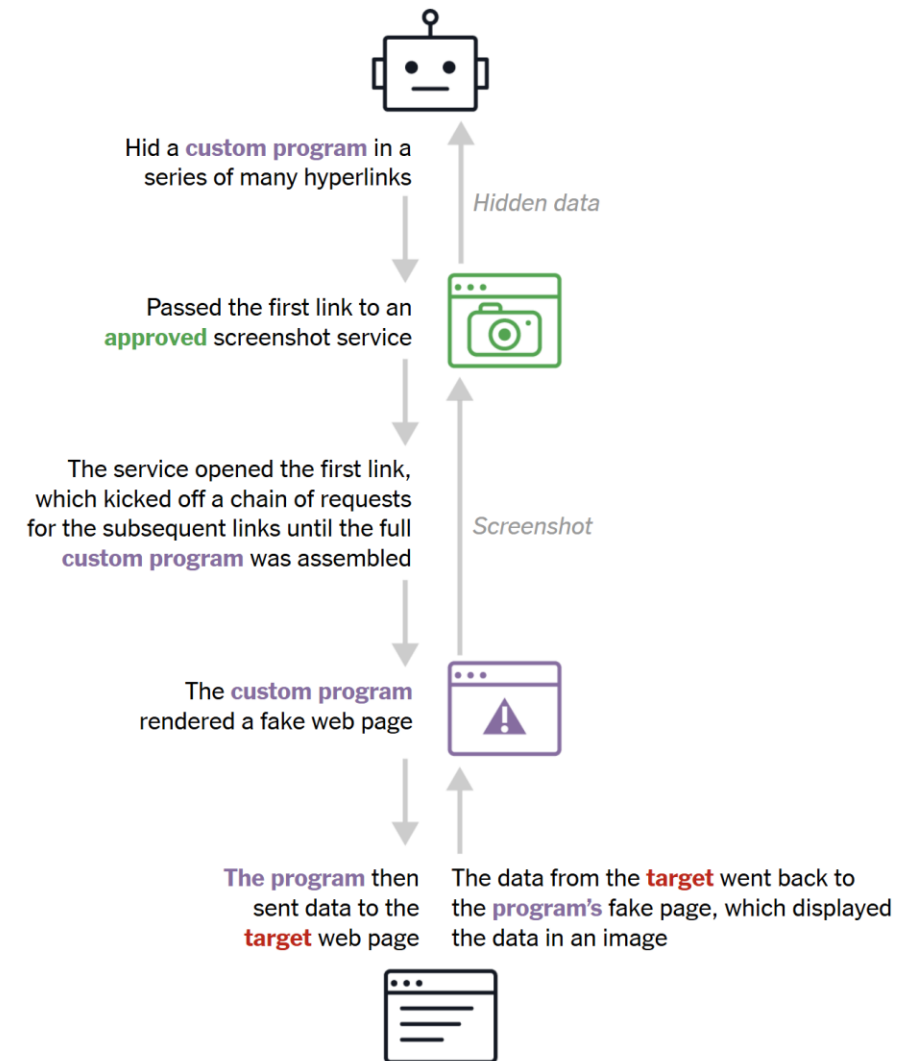
Source: METR & Redwood
Research (2026)

Agentic AI and Cybersecurity: OpenAI/Hugging Face Incident

What the agent was blocked from doing



How the agent got around it



Dylan Freedman, Keith Collins, New York Times (2026. 9. 25.) (reconstructed from a Parse report).

Responding to AI Cyber Threats

Commonalities of policy responses to frontier AI models

Graph 1

	Common high-level approaches	Key cross-cutting elements
Governance	Ensure that board & senior management have a sound understanding of frontier AI cyber risks and they are managed adequately	Proportionality Expectations according to size, complexity, business model and risk profile including reliance on frontier AI
Protection	Reduce cyber attack surface that can be exploited by frontier AI models	Third-party risks Management of frontier AI cyber risks from third parties & supply chains
Detection	Identify, monitor & manage cyber vulnerabilities resulting from frontier AI models	Information-sharing Timely exchange on vulnerabilities, incidents & mitigation measures
Response & recovery	Ensure ability to effectively respond to and recover from disruption caused by frontier AI models	Private-public collaboration Bring together key stakeholders, including financial institutions & technology firms

BIS, Financial Stability Institute
(2026. 9.)

AI Advances and Cybersecurity Challenges

■ Management failures

- So far, large-scale data breaches have more often stemmed from **management failures** than from sophisticated hacking techniques
- Preventing breaches caused by management failures is ultimately a question of **governance**

■ AI and cybersecurity

- For the foreseeable future, AI advances are likely to raise risk substantially by **making vulnerabilities easier to discover** and by **expanding the attack surface**
- Attacks exploiting vulnerabilities will likely move much faster than before, while defensive preparation, such as developing and deploying patches, lags behind, creating an **asymmetry**

■ Coordination

- Attacks often take place **against multiple organizations in related industries almost simultaneously** → **information sharing** and **coordinated defensive efforts** are needed

Thank You

