



AI Deployment and Cybersecurity in the Financial Sector: Strengthening Resilience and Supervisory Responses

2026 G20 Global Financial Stability Conference

Session 2: Financial Stability Risks and Policy Challenges from AI Innovation

27 October 2026

Fatos KOC
Head of Financial Markets Unit
Capital Markets and Financial Institutions Division
DAF, OECD



Outline

- AI in Finance: Opportunities and Emerging Cyber Threats
- Cyber Vulnerabilities and Risk Transmission
- Regulatory and Supervisory Approaches to AI in Finance
- Strengthening Cyber Resilience in the Financial System

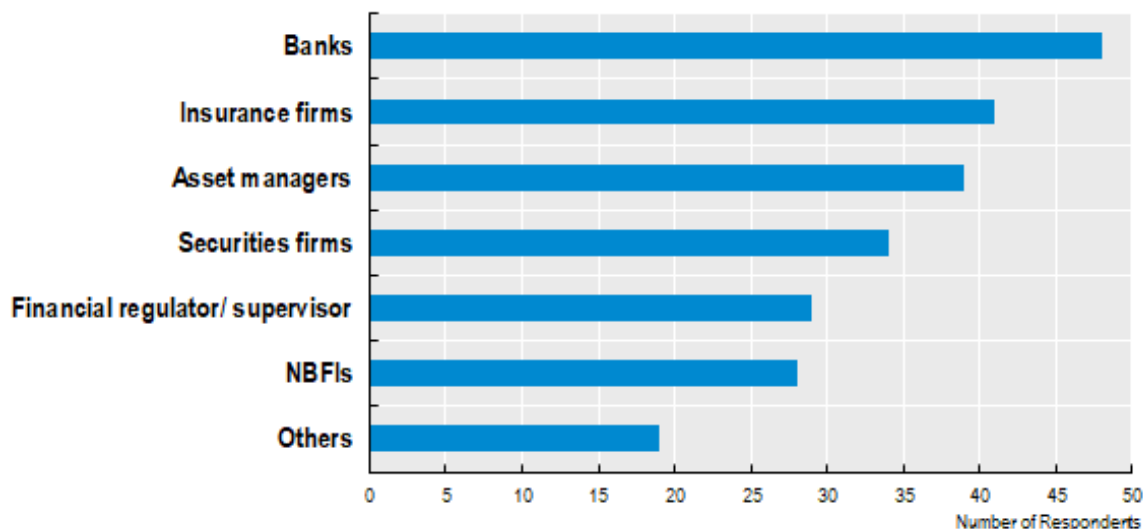




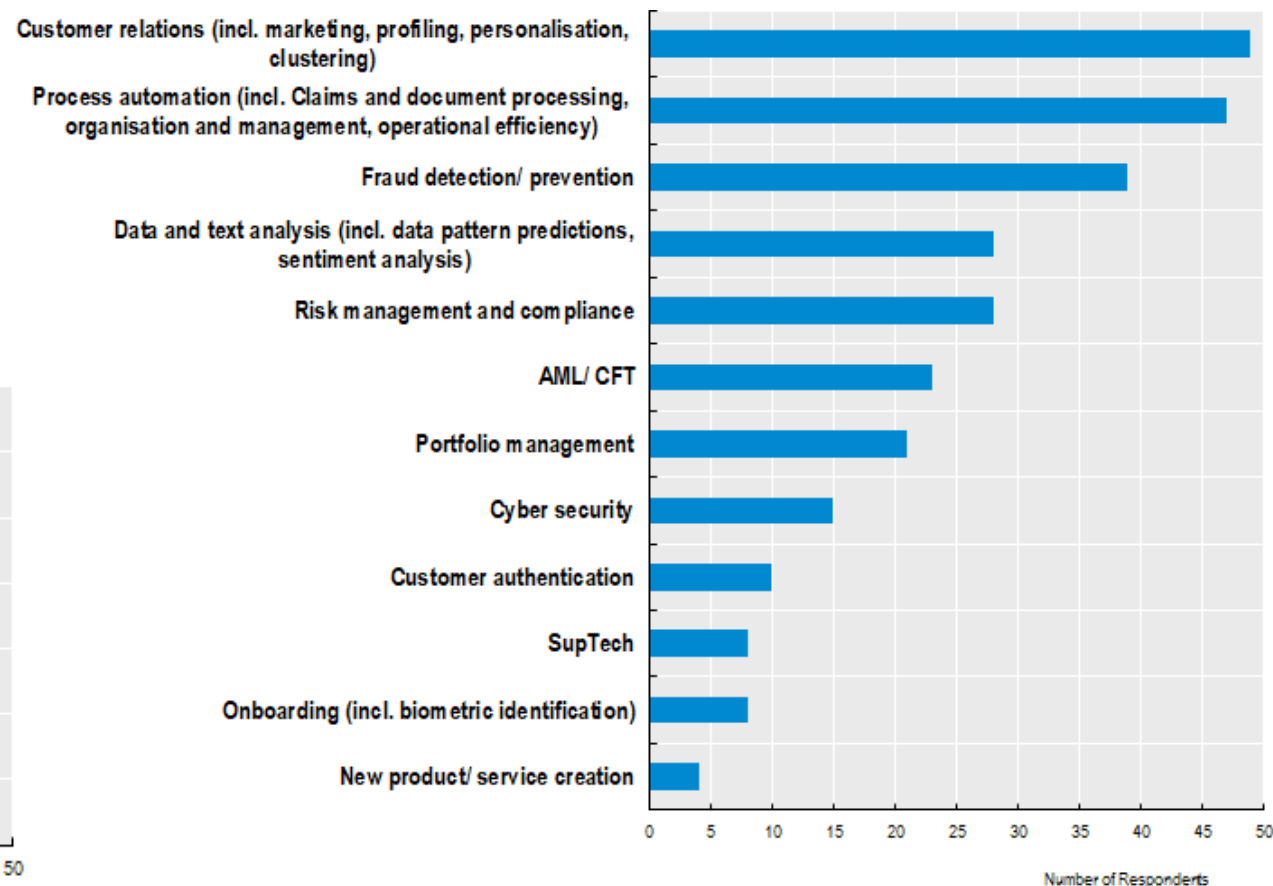
Widespread deployment of AI across financial sector

Impact on the functioning, efficiency, and integrity of financial markets across sectors of activity

Indicative types of financial firms currently experimenting with or deploying AI



Use cases and tasks involving the use of AI in finance





Generative AI: the inflection point, but slower-paced deployment in finance

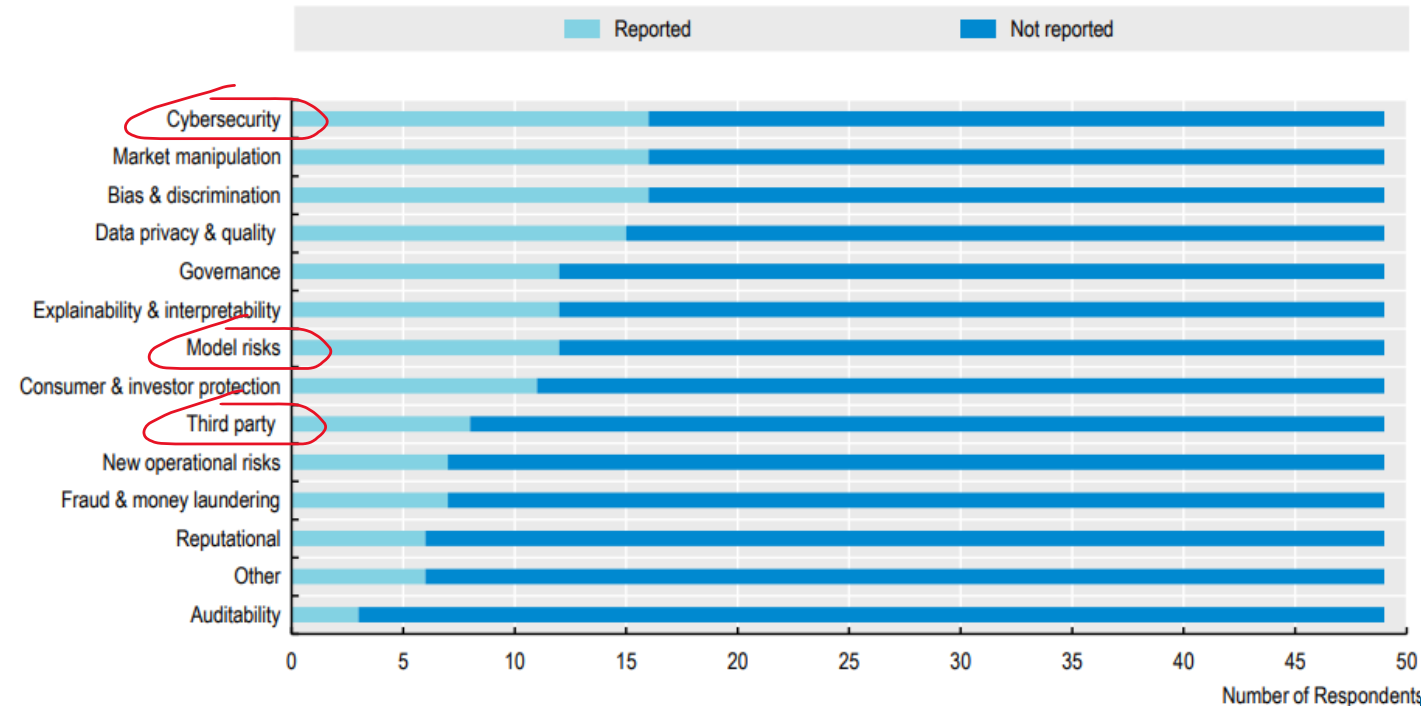
- **AI (incl. GenAI) can have a transformational impact**

- **Productivity** gains
- Real economy **growth**

Slower-paced deployment of GenAI

- “Assist” and “support” rather than full automation
- **GenAI exacerbates** financial and non-financial risks around AI use in Finance

Financial sector risks related to the use of AI in finance



Source: (OECD, 2024) Regulatory approaches to Artificial Intelligence in finance, as reported by 49 jurisdictions responding to the OECD survey.



Emergence of agentic AI could create high-value synergies, but...

Opportunities:

- ❖ Autonomous decision-making for trading, lending, and investment
- ❖ Hyper-personalised financial products and services
- ❖ Real-time risk monitoring and operational efficiencies
- ❖ Innovative financial strategies and new business models

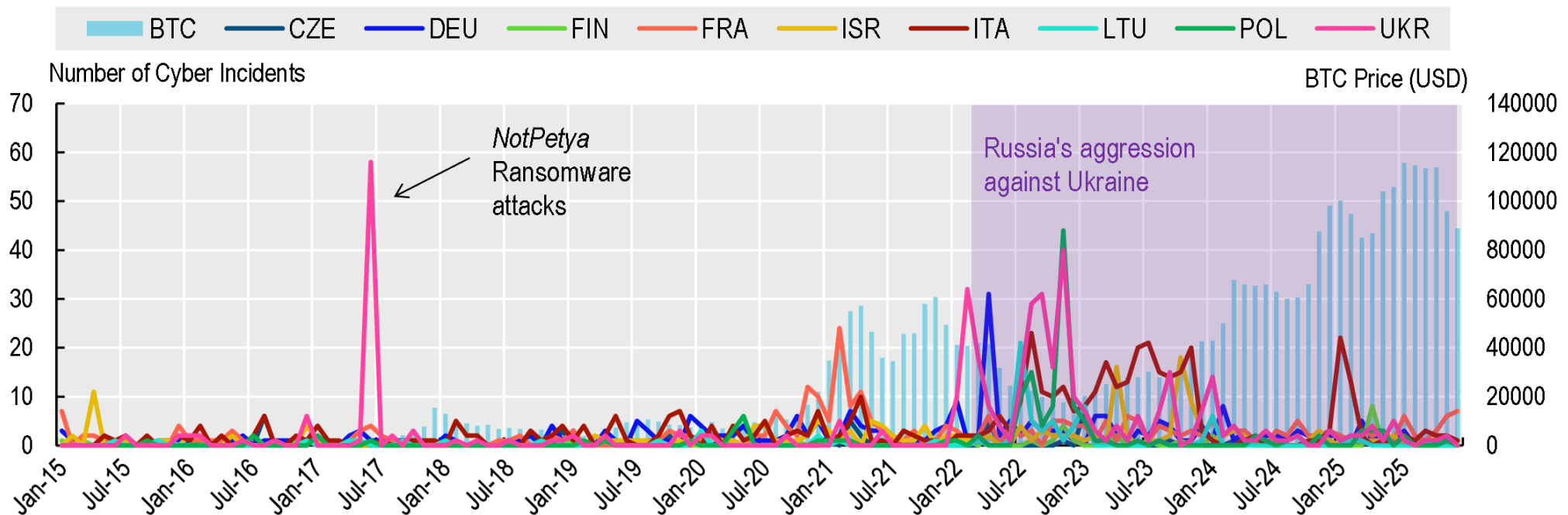
Risks:

- ❖ Amplification of systemic risks and unintended consequences
- ❖ Complexities in accountability and regulatory oversight
- ❖ Data governance, privacy, and cybersecurity concerns



Surge in cyber incidents

- Cyber incidents are increasing in frequency, scale, and sophistication, with geopolitical tensions and rapid digitalisation across the financial system.



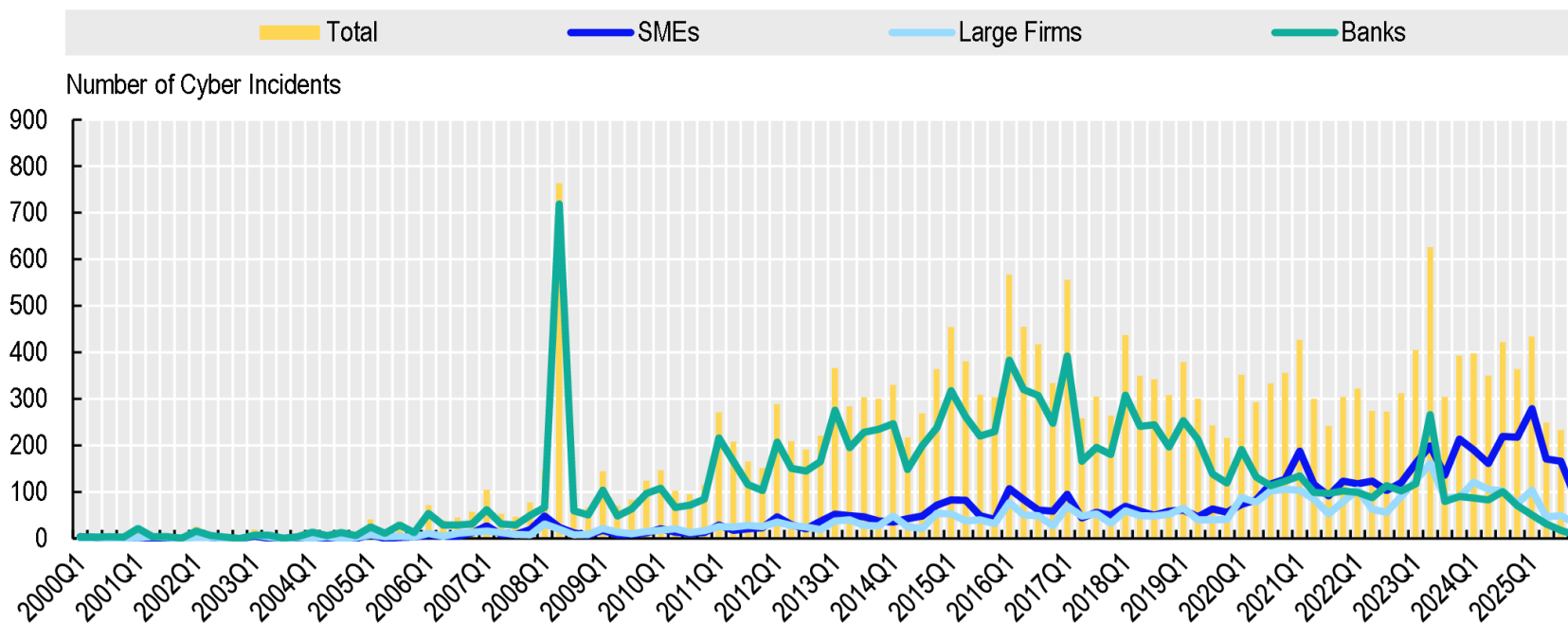
Note: The Cyber Events Database collects publicly available information on cyber events from 2014 onwards. It was created to address the lack of consistent, well-structured data necessary for making strategic decisions about how to invest resources to prevent and respond to cyber events.

Source: Yahoo Finance (<https://fr.finance.yahoo.com/>) for BTC price, Center for International & Security Studies at Maryland, Cyber Events Database with the OECD staff compilation.



Compositional shift in recent cyber incident patterns in G7

- Cyber events affecting small and medium-sized enterprises (SMEs) have risen sharply—more than fourteen-fold by 2025Q1 relative to 2021Q1 in G7 breakdowns.
- In recent quarters, SMEs record more incidents than banks.



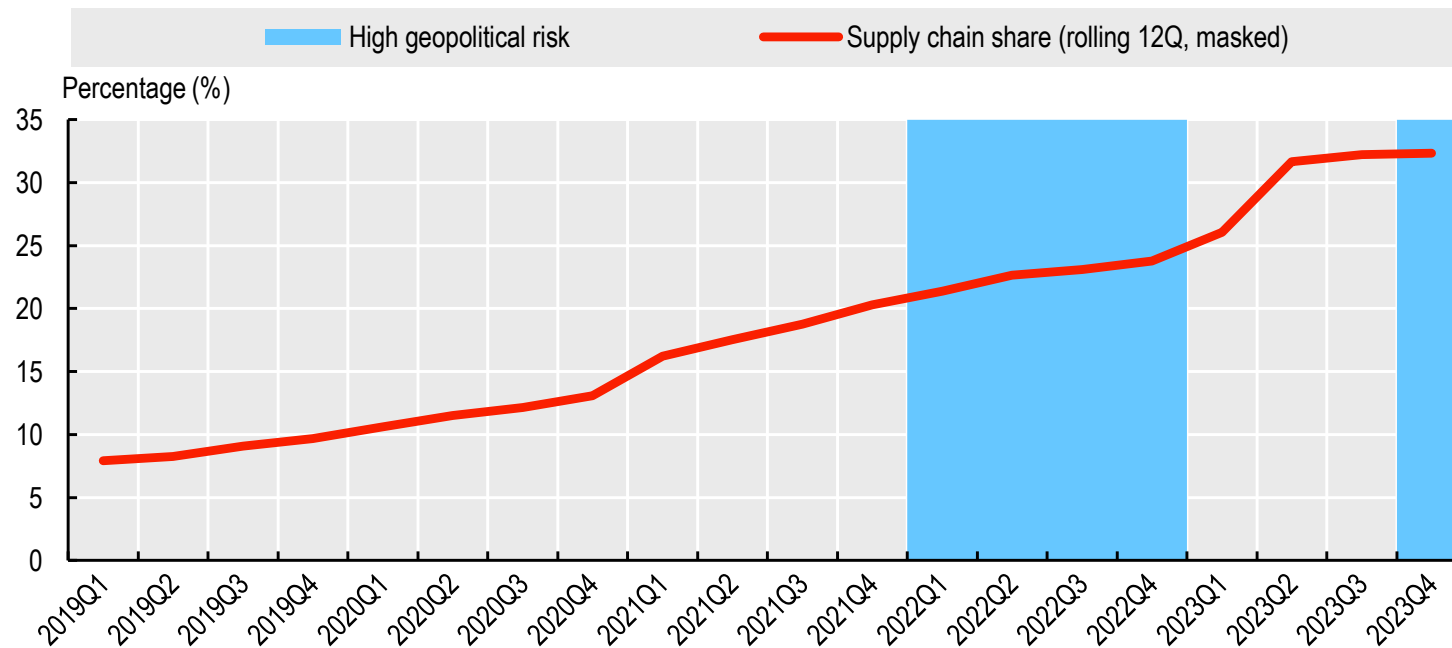
Note: Data are from the Advisen (Zywave) cyber incident database and OECD calculation. Based on NAICS 21 (Mining), 22 (Utility), 31-33 (Manufacturing), SMEs are defined as firms with fewer than 250 employees; Large Firms are those with 250 employees or more. Banks are identified as entities classified under NAICS 522 (Credit Intermediation and Related Activities). Series are quarterly counts of recorded cyber incidents. The most recent quarters may be subject to reporting lags and should be interpreted with caution.

Source: Advisen/Zywave Cyber Loss Insight feed; OECD calculations.



Deeply embedded in third-party and supply-chain

- Attacks on resource-constrained firms can provide pathways into financial institutions and propagate operational disruptions through shared infrastructures and regional value chains, especially when cyber activity interacts with geopolitical risk.



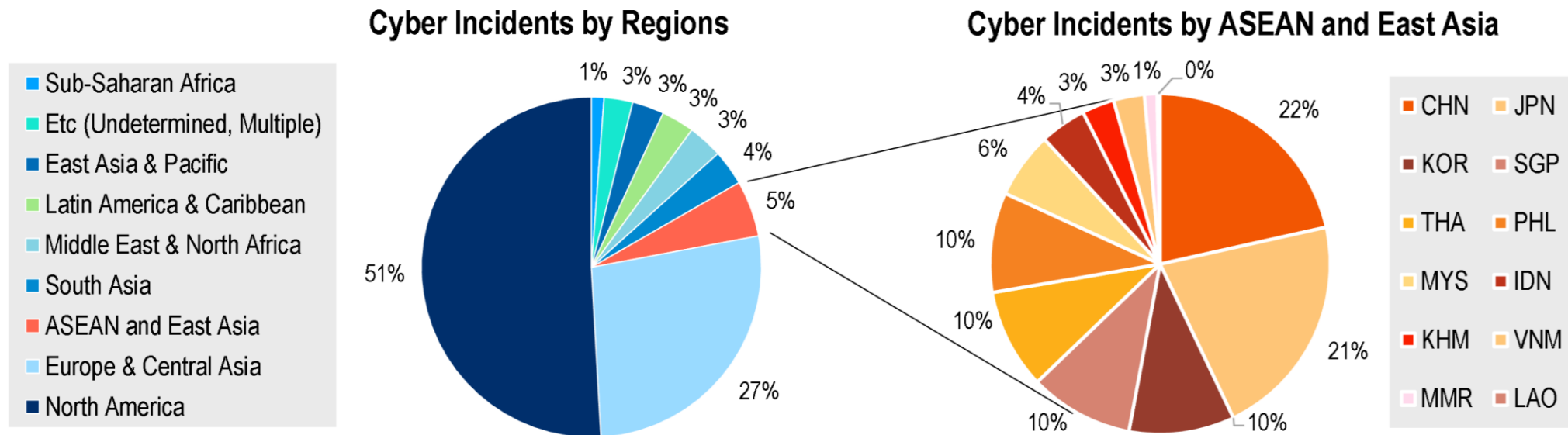
Note: In this chart, “supply chain-related” incidents refer to incidents affecting critical ICT and service dependencies relevant to financial institutions. Data are from the Zywave/Advisen Standard Cyber Loss Insight Feed and OECD calculations. The red line plots the share (%) of cyber incidents affecting financial institutions that are classified as third party/vendor related, computed as a 12 quarter (3 year) rolling share. Shaded areas indicate quarters of high geopolitical risk, defined as quarters in the top quartile of the quarterly average Geopolitical Risk (GPR) index from Caldara and Iacoviello (2022) (data downloaded on April 9, 2026).

Source: Caldara, Dario and Matteo Iacoviello (2022), “Measuring Geopolitical Risk,” American Economic Review, April, 112(4), pp.1194-1225.; Zywave/Advisen Standard Cyber Loss Insight Feed and OECD calculations.



ASEAN as a focal lens where high SME prevalence

- Uneven cyber maturity, and cross-border interdependencies in ASEAN can amplify vulnerabilities, while cyber-enabled financial crime risks are also evolving in parts of ASEAN.



Note: The Cyber Events Database collects publicly available information on cyber events, beginning in 2014 to the present day. It was created to address a lack of consistent, well-structured data necessary for making strategic decisions about how to invest resources to prevent and respond to cyber events.

Source: Center for International & Security Studies at Maryland, Cyber Events Database with the OECD staff compilation.



From preparedness to cyber resilience

- **Ex-ante vs ex-post (focus & timing)**
 - Ex-ante (before): identify vulnerabilities and reduce exposure (scenario analysis, cyber stress testing, mutual evaluations, better data).
 - Ex-post (after): **‘after-the-event’** response, containment, recovery, and AML/CFT.
- **Why ex-ante is critical in cybersecurity**
 - Precautionary protection (ex-ante): baseline hygiene, access controls, credential protection such as private keys, and incident response readiness.
 - Strengthening baseline security, third-party oversight, regional cooperation, and forward-looking assessment capabilities is essential to reduce systemic fragility, maintain market confidence, and protect financial stability.



Existing financial regulations address many AI-related risks

❖ Appropriate regulation in place in the vast majority of 49 jurisdictions examined

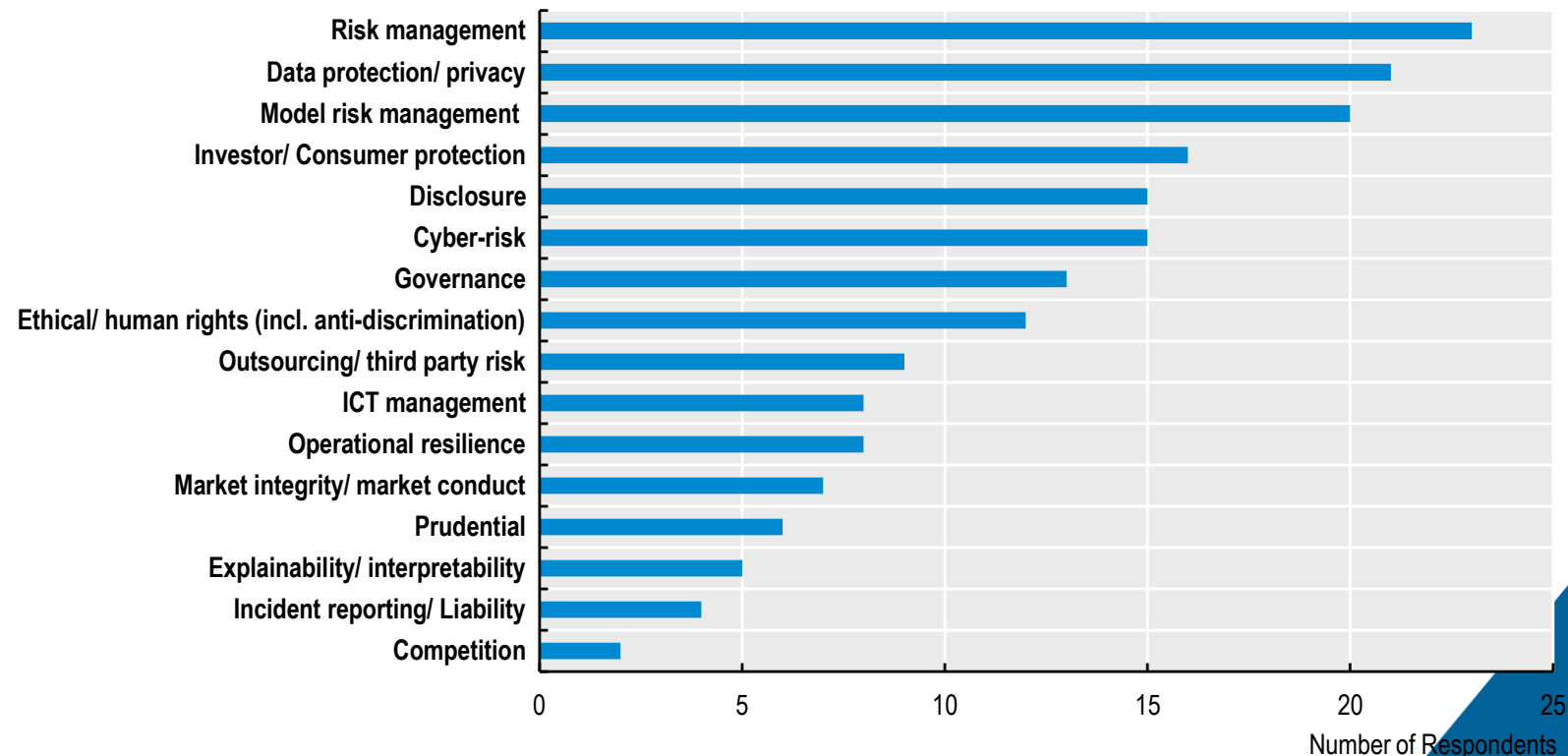
- pre-existing rules or new regulation;
- binding or non-binding rules;
- finance-specific or cross-sectorial

❖ Existing financial regulation, laws and guidance applies

❖ Technology-neutral approach

- Proportional/ risk-based

Indicative examples of areas covered by existing financial sector rules



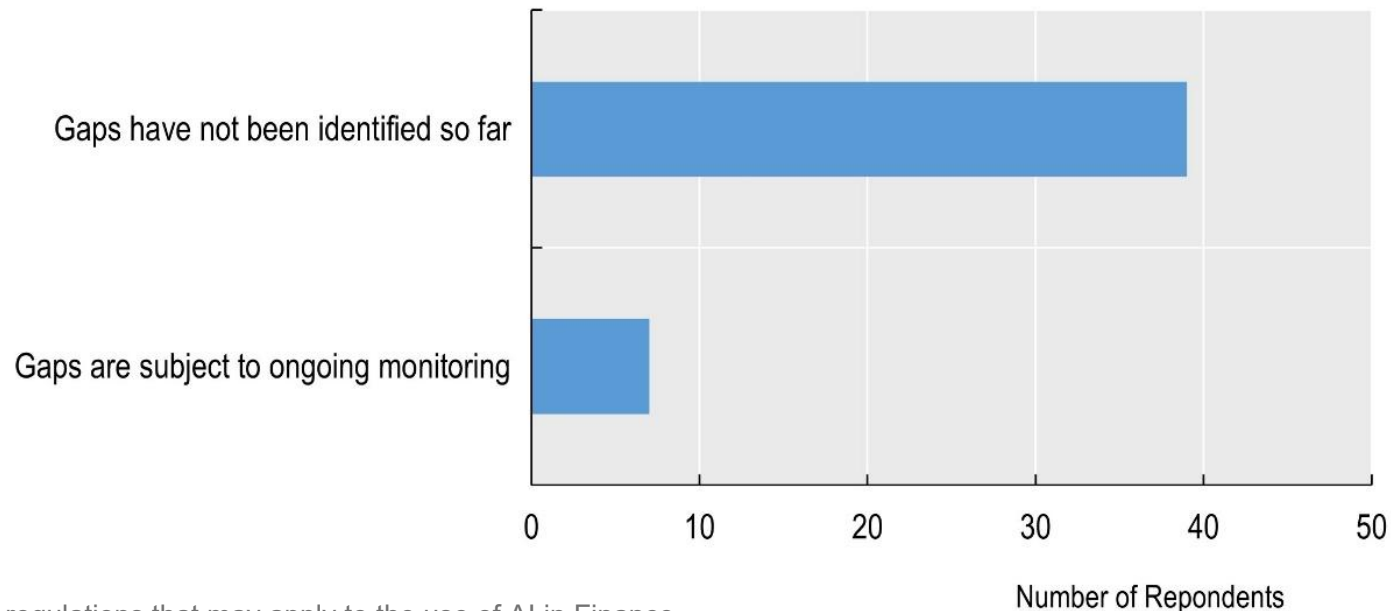
Source: (OECD, 2024) Regulatory approaches to Artificial Intelligence in finance, as reported by 49 jurisdictions responding to the OECD survey.



Ongoing monitoring and reviews to ensure frameworks remain fit-for-purpose

- ❖ No gaps to the current regulatory and supervisory framework applicable to AI in finance identified in the majority of respondent jurisdictions
 - ***But continuous ongoing monitoring and investigation***
- ❖ Reviewing existing regulatory frameworks to **ensure they remain fit for purpose**

Potential gaps identified by financial regulators to existing rules on AI in finance



Note: Non-exhaustive examples of rules and regulations that may apply to the use of AI in Finance.
Source: 2024 OECD Survey on Regulatory Approaches to AI in Finance.



Enhancing cyber resilience: policy implications

International cooperation and information sharing

- Promote greater consistency in cyber incident reporting and cross-border information sharing.
- OECD AI incident reporting supports information-sharing, improving collective resilience and supervisor coordination

Public-private collaboration and Supervisory capacity

- Co-develop standards, invest in skills, and leverage industry and academic expertise into regional analytical hubs using shared cyber-incident and financial data.
- Strengthen supervisory expertise and understanding of AI dependencies, third-party concentration and evolving cyber threats.

Testing, preparedness and systemic resilience

- Conduct cyber resilience exercises and scenario-based testing, including AI-enabled attacks and disruptions to critical service providers.
- Strengthen incident response, recovery arrangements and cross-sector coordination to contain systemic spillovers.



THANK YOU

Find more online:

<https://www.oecd.org/en/topics/sub-issues/digital-finance.html>

OECD (2024), “Regulatory approaches to Artificial Intelligence in finance” <https://doi.org/10.1787/f1498c02-en>.

OECD (2026), “Cybersecurity and Geopolitical Risks in Financial Markets” <https://doi.org/10.1787/1002b1fd-en>

OECD (2026), “Supervision of artificial intelligence in finance: Challenges policies and practices”
<https://doi.org/10.1787/92743dc1-en>

OECD (2022), “OECD Policy Framework on Digital Security: Cybersecurity for Prosperity”
<https://doi.org/10.1787/a69df866-en>.

[OECD \(2022\), “Recommendation of the Council on the Treatment of Digital Security Vulnerabilities”](#)
[OECD Legal Instruments](#)