Banking and Capital Markets bi-weekly news round-up

9 May 2025
Edition no: 335

Contents

Welcome to the DXC-curated news round-up.

A collection of technology-related articles for banking and capital markets (BCM). DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds.

With this news round-up, published every 2 weeks, we highlight innovative and emerging news, regulation and research, as well as including DXC thought-leadership that explores new ideas, technologies and best practices.

To thrive in the complex and competitive financial market, banking and capital markets firms need products and services that work for twenty-first century customers and meet regulatory obligations. Modernise your IT and transform your business with DXC Technology's IT services and robust partner ecosystem.

Should you have any comments or suggestions, please feel free to contact me.

Happy reading.

Jean-Paul Simoes

Director of Banking and Capital Markets (BCM) Compliance, DXC Technology

jean-paul.simoes@dxc.com

Learn more at: dxc.com/UK/banking

What's in store for banking in 2025?

New DXC publication: We (continue to) live in interesting times. In 2025, banks will need to deal with issues related to security, the rapid adoption of new technologies (i.e., GenAI-based processes), the ongoing maturity of digitization initiatives (e.g., the UK government's digital Driver's License/Digital ID program), and (potentially the most disruptive) the rapidly evolving geo-political risks that are emerging. Wars (e.g., Ukraine, Gaza), dramatic climate events (e.g., L.A. fires, Spanish floods), inflation, recession, and numerous other challenges will continue to contribute to the uncertainty of the banking environment. If the Executive Orders signed by President Trump on his first day teach us anything, it is that we can no longer take for granted any consistency of policies from one administration to the next.

2025 will be action-packed and unpredictable. DXC Technology builds and runs the world's mission-critical systems. We're entrusted with developing, building, securing, and innovating these systems to meet the critical and evolving needs of our clients and the communities we serve.

Resilience and security are embedded in our DNA thanks to our expert delivery teams, AI experts, and solution engineers. DXC Technology is well placed to work collaboratively with our clients as they navigate the challenges ahead in 2025.

Artificial Intelligence (AI)

What are the risks from Artificial Intelligence?

MIT: The risks posed by Artificial Intelligence (AI) are of considerable concern to academics, auditors, policymakers, AI companies, and the public. However, a lack of shared understanding of AI risks can impede our ability to comprehensively discuss, research, and react to them.

This paper addresses this gap by creating an AI Risk Repository to serve as a common frame of reference. This comprises a living database of 1612 risks extracted from 65 taxonomies, which can be filtered based on two overarching taxonomies and easily accessed, modified, and updated via our website and online spreadsheets. We construct our Repository with a systematic review of taxonomies and other structured classifications of AI risk followed by an expert consultation. We develop our taxonomies of AI risk using a best-fit framework synthesis.

Our high-level Causal Taxonomy of AI Risks classifies each risk by its causal factors (1) Entity: Human, AI; (2) Intentionality: Intentional, Unintentional; and (3) Timing: Pre-deployment; Post-deployment. Our mid-level Domain Taxonomy of AI Risks classifies risks into seven AI risk domains: (1) Discrimination & toxicity, (2) Privacy & security, (3) Misinformation, (4) Malicious actors & misuse, (5) Human-computer interaction, (6) Socioeconomic & environmental, and (7) AI system safety, failures, & limitations.

Why AI Benchmarks are an 'Illusion'

404 Media: Chatbot Arena is the most popular AI benchmarking tool, but new research says its scores are misleading and benefit a handful of the biggest companies.

The most popular method for measuring what are the best chatbots in the world is flawed and frequently manipulated by powerful companies like OpenAI and Google in order to make their products seem better than they actually are, according to a new paper from researchers at the AI company Cohere, as well as Stanford, MIT, and other universities.

The researchers came to this conclusion after reviewing data that's made public by Chatbot Arena (also known as LMArena and LMSYS), which facilitates benchmarking and maintains the leaderboard listing the best large language models, as well as scraping Chatbot Arena and their own testing. Chatbot Arena, meanwhile, has responded to the researchers findings by saying that while it accepts some criticisms and plans to address them, some of the numbers the researchers presented are wrong and mischaracterize how Chatbot Arena actually ranks LLMs. The research was published just weeks after Meta was accused of gaming AI benchmarks with one of its recent models.

DXC Technology Banking and Capital Markets bi-weekly news round–up

IT leaders see big business potential in small AI models

CIO: Better equipped to deliver business-specific AI apps, small language models (SLMs) could soon outpace LLM use in the enterprise, thanks to their agile, cost-efficient, task-targeted nature.

Small language models (SLMs) are giving CIOs greater opportunities to develop specialized, business-specific AI applications that are less expensive to run than those reliant on general-purpose large language models (LLMs).

By 2027, smaller, context-specific models will outpace their counterparts with usage volume at least three times more than those of LLMs, according to a recent report from Gartner, which also claims LLM response accuracy declines for tasks requiring specific business context.

"The variety of tasks in business workflows and the need for greater accuracy are driving the shift towards specialized models fine-tuned on specific functions or domain data," says Sumit Agarwal, an analyst at Gartner who helped author the report. "These smaller, task-specific models provide quicker responses and use less computational power, reducing operational and maintenance costs."

Hallucination is Inevitable: An Innate Limitation of Large Language Models

Cornell University: Hallucination has been widely recognized to be a significant drawback for large language models (LLMs). There have been many works that attempt to reduce the extent of hallucination. These efforts have mostly been empirical so far, which cannot answer the fundamental question whether it can be completely eliminated.

In this paper, we formalize the problem and show that it is impossible to eliminate hallucination in LLMs. Specifically, we define a formal world where hallucination is defined as inconsistencies between a computable LLM and a computable ground truth function. By employing results from learning theory, we show that LLMs cannot learn all the computable functions and will therefore inevitably hallucinate if used as general problem solvers. Since the formal world is a part of the real world which is much more complicated, hallucinations are also inevitable for real world LLMs.

Furthermore, for real world LLMs constrained by provable time complexity, we describe the hallucination-prone tasks and empirically validate our claims. Finally, using the formal world framework, we discuss the possible mechanisms and efficacies of existing hallucination mitigators as well as the practical implications on the safe deployment of LLMs.

DXC Technology Banking and Capital Markets bi-weekly news round–up

DXC perspective

JPMorgan's 2025 AI report is less about trends and more of a manifesto.

On payments, I see this as a market reset. Their approach to "Agentic AI" isn't about operational efficiency, it's redefining what customers expect across the lifecycle: Payments, Lending, Advice, and even non-banking tasks like travel.

Most banks are still tuning legacy core platforms. JPM is designing systems that think, act, and transact before a customer clicks. That's not innovation — that's a paradigm shift.

The risk? AI inequality becomes existential.

If your roadmap doesn't include embedded intelligence across customer journeys, you're not catching up — you're falling behind.

Suneet Mutta, FSI UK&I, DXC Technology.

DXC perspective

The article highlights the alarming ease with which AI enables sophisticated and targeted attacks by less sophisticated attackers, increasing both their number and difficulty to detect. AI's ability to create culturally relevant and individualized phishing emails significantly enhances the effectiveness of these malicious campaigns, outpacing traditional detection technologies.

Preventive Measures:
Even the most diligent staff can miss sophisticated phishing attempts, but a combination of training and awareness campaigns, along with robust layered security measures, can significantly mitigate these risks. Implementing a Zero Trust Cyber Security Strategy, which includes Multi-factor Authentication, Network Segmentation, and Continuous Monitoring with AI tools, is essential to protect against these advanced threats.

Andrew Shephard, EMEA Banking Security, DXC Technology.

Bank Sector

JPM's 2025 Emerging Technology Trends: All GenAI, All the Time

Cashless: JPMorganChase (JPM) is renowned for its use of AI, and if you read no other document about AI and banking this year, make it this one, it's that good! JPM's 2025 Emerging Technology Trends is poorly named as the report isn't about "trends," plural, but is 100% devoted to AI and contains use cases that are nothing short of state-of-the-art.

The real issue isn't the fantastic vision that JPM is showing with its proposed AI use. It is what happens with all of the other banks that are woefully behind?

If you read this report to see what JPM is working on, and still discount it by half as corporate propaganda, they are miles ahead of most large and medium banks anywhere in the globe. The gap, or what I like to refer to as "AI inequality," is so large that I think the best many banks can hope for is to stay in the middle of the pack. Those lingering far behind will simply have a hard time surviving.
As for Agentic AI, it will be in use everywhere, from financial transactions and advertising to software development and cybersecurity. It is foundational technology.

Cyber Security

Ex-NSA cyber-boss: AI will soon be a great exploit coder

The Register: RSAC Former NSA cyber-boss Rob Joyce thinks today's artificial intelligence is dangerously close to becoming a top-tier vulnerability exploit developer. "At RSAC last year, I told people: 'Don't worry about the zero-day AI Armageddon,' but I am increasingly worried that AI is going to be a good bug finder this year, [and] an exploit developer in the near future," the retired Director of the NSA's Cybersecurity Directorate told *The Register* during an interview this week at the RSA Conference in San Francisco.

How near is the near future? Either this year or next, predicted Joyce, who now serves as an advisor to Sandfly Security, a supplier of intrusion detection tools for Linux systems.

"All the frontier models have got very good at coding," Joyce noted. "In fact, OpenAI models are out-competing humans in many of the code competitions."

Case in point: The Hack The Box capture-the-flag contest earlier this month during which AI-powered entrants performed at about the same speed as pure-human teams, and nearly matched humans in tests of problem-solving ability.

By the end of the contest, the top AI team captured 19 of 20 flags, placing 20th out of 403 teams with 15900 points; most of the AI teams captured 19 flags in fact.

Regulatory

The SEC and DOJ Signal Continued Focus on AI Washing Under Trump Administration

Debevoise: On April 9, 2025, the U.S. Securities and Exchange Commission (the "SEC") and the U.S. Attorney's Office for the Southern District of New York filed parallel actions against Albert Saniger, the former CEO of Nate, Inc. ("Nate"), alleging that he made materially false and misleading statements to investors about the company's artificial intelligence ("AI") capabilities.

This matter is particularly noteworthy as the cases are the first AI-washing enforcement actions brought by the SEC and Department of Justice ("DOJ") under the new Trump administration. These actions demonstrate that the SEC and DOJ intend to continue pursuing both civil and criminal charges against individuals for alleged misstatements or omissions concerning the use of AI—including in the context of private market fundraising.

DOJ's indictment and the SEC's civil complaint allege that Saniger raised over $42 million from private market investors by falsely claiming that Nate's mobile shopping software used AI to complete users' purchases across a variety of retail platforms. According to the government's filings, Saniger solicited investments by touting Nate's purported reliance on AI—including "machine learning" and "neural networks"—to autonomously process transactions, when in fact he knew that virtually all of the purchases were being completed manually by contract workers based in the Philippines, Romania, and elsewhere

China's chipmakers are catching up to Nvidia and TSMC. Here's how they compare

Rest of world: Washington's latest export restrictions on Nvidia's H20 chips are likely to accelerate China's shift toward domestic alternatives, as homegrown firms strive to close the gap with global rivals.

Years of controls on U.S. chips have pushed the Chinese government to invest billions in its domestic supply chain for semiconductors that are key to the development of artificial intelligence.

"China's progress is being slowed down by chip-related controls, but it is hard to imagine a situation where you can stop them forever," Ray Wang, a semiconductor analyst based in Washington, D.C., told *Rest of World*.

China has advanced more in some areas — such as memory chips and design — than others, while struggling with equipment making, he said.

Nvidia CEO Jensen Huang made a surprise visit to Beijing days after the U.S. announced new restrictions on the most advanced AI chip it was previously allowed to sell in China. Huang told officials he hoped to "continue to cooperate with China."

Here's how five major Chinese semiconductor companies compare to the global leaders.....

Should you have any questions on the round-up or a particular topic, please feel free to contact your DXC representative.

Learn more at:
dxc.com/UK/banking

Newsletter Disclaimer

This newsletter is intended solely for informational purposes only. It does not constitute professional advice or recommendation. Any reliance on the content is at the reader's own risk. Readers are encouraged to verify any details independently and contact relevant experts before making business decisions.

While we strive for accuracy, DXC Technology does not warrant the completeness, reliability, or timeliness of the information presented. Unauthorized distribution, reproduction, or disclosure to any third party is strictly prohibited.

DXC Technology
DXC.com

About DXC Technology

DXC Technology (NYSE: DXC) helps global companies run their mission-critical systems and operations while modernizing IT, optimizing data architectures, and ensuring security and scalability across public, private and hybrid clouds. The world's largest companies and public sector organizations trust DXC to deploy services to drive new levels of performance, competitiveness, and customer experience across their IT estates. Learn more about how we deliver excellence for our customers and colleagues at **DXC.com**.