DXC TECHNOLOGY

Banking and Capital Markets bi-weekly news round-up

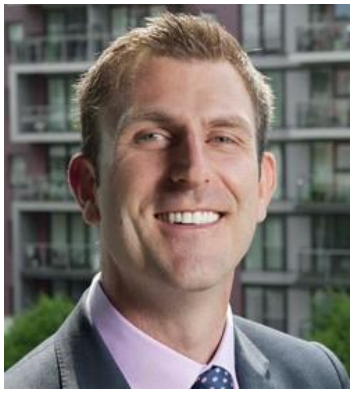
9 June 2023
Edition no: 290

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 Technology's 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

Contents

Artificial Intelligence (AI)

ChatGPT on Wall Street Could Be Disastrous, Financial History Shows

Scientific American: Using artificial intelligence like ChatGPT to trade stocks and other financial instruments could have benefits—and perils

Artificial Intelligence-powered tools, such as ChatGPT, have the potential to revolutionize the efficiency, effectiveness and speed of the work humans do. And this is true in financial markets as much as in sectors like health care, manufacturing and pretty much every other aspect of our lives.

I've been researching financial markets and algorithmic trading for 14 years. While AI offers lots of benefits, the growing use of these technologies in financial markets also points to potential perils. A look at Wall Street's past efforts to speed up trading by embracing computers and AI offers important lessons on the implications of using them for decision-making.

PROGRAM TRADING FUELS BLACK MONDAY

In the early 1980s, fueled by advancements in technology and financial innovations such as derivatives, institutional investors began using computer programs to execute trades based on predefined rules and algorithms. This helped them complete large trades quickly and efficiently.

DXC Perspective

Generative AI models such as GPT4 are massive language prediction models. The vast training set that it is trained on may make it right sometimes, while it may appear plausible at others. There are lots of wonderful uses of Large Language Models (LLMs), some of which are outlined in this article. I suspect there will be unintended consequences, too. In high-stakes, regulated situations, a layered architecture with more robust computational methods that query factual knowledgebases, feeding into an LLM as the empathetic-sounding linguistic interface, will make these AI systems more accurate, predictable, explainable and empathetic.

Zohair Gangjee
Managing Director
Banking and Capital Markets
DXC Technology

What every CEO should know about generative AI

McKinsey: Generative AI is evolving at record speed while CEOs are still learning the technology's business value and risks. Here, we offer some of the generative AI essentials.

Amid the excitement surrounding generative AI since the release of ChatGPT, Bard, Claude, Midjourney, and other content-creating tools, CEOs are understandably wondering: Is this tech hype, or a game-changing opportunity? And if it is the latter, what is the value to my business?

The public-facing version of ChatGPT reached 100 million users in just two months. It democratized AI in a manner not previously seen while becoming by far the fastest-growing app ever. Its out-of-the-box accessibility makes generative AI different from all AI that came before it. Users don't need a degree in machine learning to interact with or derive value from it; nearly anyone who can ask questions can use it.

And, as with other breakthrough technologies such as the personal computer or iPhone, one generative AI platform can give rise to many applications for audiences of any age or education level and in any location with internet access.

AI machines aren't 'hallucinating'. But their makers are

The Guardian: Tech CEOs want us to believe that generative AI will benefit humanity. They are kidding themselves

Inside the many debates swirling around the rapid rollout of so-called artificial intelligence, there is a relatively obscure skirmish focused on the choice of the word "hallucinate".

This is the term that architects and boosters of generative AI have settled on to characterize responses served up by chatbots that are wholly manufactured, or flat-out wrong. Like, for instance, when you ask a bot for a definition of something that doesn't exist and it, rather convincingly, gives you one, complete with made-up footnotes. "No one in the field has yet solved the hallucination problems," Sundar Pichai, the CEO of Google and Alphabet, told an interviewer recently.

That's true – but why call the errors "hallucinations" at all? Why not algorithmic junk? Or glitches? Well, hallucination refers to the mysterious capacity of the human brain to perceive phenomena that are not present, at least not in conventional, materialist terms.

If you don't have a Generative AI strategy, it's time to get one

DXC: An article about how to prepare a smart and responsible Generative AI strategy and start using the technology now

Now is the time to get started with generative artificial intelligence (AI) – especially because your competition is most likely using the technology already or planning to use it soon.

Need proof? Consider this: In a survey recently conducted by Scale AI, more than 8 in 10 business leaders said they either have Generative AI already in production or are planning to use or experiment with the technology soon.

For further evidence, consider the rapid adoption of the ChatGPT chatbot, software that uses Generative AI. In just the first week after ChatGPT launched, it gained over 1 million users.

Since then, ChatGPT has attracted more than 100 million users who generate some 10 million queries daily. While these figures undoubtedly include some nonbusiness users, they nonetheless point to the high level of interest that Generative AI has, well, generated. ChatGPT has also spawned competitors and collaborators that are rushing to capture market share, test functionality or embed it in their own offerings.

Cybersecurity

Lessons from The Financial Stability Board's Report on Cyber Incident Reporting

Debevoise & Plimpton Data Blog: Big businesses, especially those with a global footprint and operating in regulated sectors, are increasingly confronted with new and diverging cyber incident reporting requirements.

A single incident—even a relatively minor one—may require notification to dozens of data protection, cyber, law enforcement, and sectoral regulators around the world, in addition to insurers, customers, and counterparties. Not only do many regulatory reporting obligations have materially different triggers, but also significant variation exists in reporting timeframes, content requirements, and subsequent regulatory engagement practices.

The cumulative effect of this regulatory spiderweb of red tape is often to divert attention and resources away from substantive incident response and remediation, and to create a bureaucratic vortex for compliance and legal personnel. To make matters worse, businesses cannot simply hire their way out of this morass. With a ~3.4 million person shortage in information security professionals, when regulators force too much attention on incident reporting they are invariably diverting eyes from actual information security.

Large Spanish bank confirms ransomware attack

The Record: A major lender in Spain said it is dealing with a ransomware attack affecting several offices.

Globalcaja – based in the Spanish city of Albacete – has more than 300 offices across Spain and serves nearly half a million people with a variety of banking services. It manages more than $4.6 billion in consumer loans and has 1,000 employees.

The Play ransomware group claimed this week that it attacked the bank and stole an undisclosed amount of private and personal confidential data, client and employee documents, passports, contracts and more.

The bank published a statement on Friday confirming that computers at several local offices were dealing with ransomware.

"It has not affected the transactions of the entities (nor the accounts or the agreements of clients.) The offices are operating with total normality when it comes to electronic banking and ATMs," they said in a statement.

"From the very beginning, at Globalcaja we activated the security protocols created for this purpose, which led us to disable some office posts and temporarily limit the performance of some operations. We continue to work hard to finish normalizing the situation and are analyzing what happened, prioritizing security at all times. We apologize for any inconvenience caused."

Fancy Bear Goes Phishing by Scott Shapiro, review – a gripping study of five extraordinary hacks

The Guardian: A professor of law who's a computer geek carves an undaunted path through the conceptual and technical undergrowth in this illuminating tour of cyberspace's dark side

As we head towards 2030, a terrible realisation is dawning on us – that we have built a world that is critically dependent on a set of technologies that almost nobody understands, and which are also extremely fragile and insecure. *Fancy Bear Goes Phishing* seeks to tackle both sides of this dilemma: our collective ignorance, on the one hand, and our insecurity on the other. Its author says that he embarked on the project seeking an understanding of just three things. Why is the internet so insecure? How (and why) do the hackers who exploit its vulnerabilities do what they do? And what can be done about it?
In ornithological terms, Scott Shapiro is a pretty rare bird – an eminent legal scholar who is also a geek. Wearing one hat (or perhaps a wig), he teaches jurisprudence, constitutional law, legal philosophy and related topics to Yale students. But wearing different headgear (a reversed baseball cap?), he is also the founding director of the university's cybersecurity lab, which does pretty good research on security and information technology generally.

The Quantum Computing Threat Is Just a Matter Of Time

Oliver Wyman: Predictions vary but the need to prepare is real and present

Quantum computing is advancing rapidly from being a physics problem to an engineering challenge that could revolutionize technology for the benefit of mankind, but also potentially pose a significant threat to data security. For decades, hackers have persisted in the pursuit of valuable data, typically encrypted, with Shor's algorithm (a computing method that can solve complex math problems related to factoring large numbers, which has important applications in encryption and security). This level of encryption through classical computing methods can tire and ultimately thwart those with malicious intent however, quantum computing has the potential to dramatically change the game.

The reality of the quantum threat

Current hardware limitations represent a thorn in the side of advancing quantum capabilities and a prime factor in sowing doubt about the potential for quantum computers to compromise public-key encryption. While experts disagree on the timeline for quantum computers to achieve the qubit counts and stability necessary to threaten public-key encryption, it is clear that companies need to prepare for the possibility of a quantum-enabled cyberattack.

Ransomware corrupts data, so backups can be faster and cheaper than paying up

The Register: Smash and grab raids don't leave time for careful encryption

Ransomware actors aim to spend the shortest amount of time possible inside your systems, and that means the encryption they employ is shoddy and often corrupts your data. That in turn means restoration after paying ransoms is often a more expensive chore than just deciding not to pay and working from our own backups.

That's the opinion of Richard Addiscott, a senior director analyst at Gartner.

"They encrypt at excessive speed," he told the firm's IT Infrastructure, Operations & Cloud Strategies Conference 2023 in Sydney on 15 May. "They encrypt faster than you can run a directory listing."

Ransomware operators therefore encrypt badly and lose some of the data they then try to sell you back.

Restoring from corrupt data dumps delivered by crooks is not easy, Addiscott advised – and that's if ransomware operators deliver all the data they promise. Plenty don't – instead they use a ransom payment to open a new round of negotiations about the price of further releases.

4 Areas of Cyber Risk That Boards Need to Address

Note: Accessing this article requires a subscription.

HBR: In our technology-dependent society, the effectiveness of cyber risk governance of companies affects its stock prices, as well as short-term and long-term shareholder value. New SEC cybersecurity rules provide a solid basis for transparency. Unfortunately, monitoring the long-term effectiveness of a cyber risk management strategy is not easy to grasp. This article provides four critical areas investors should be informed about for evaluating its long-term effectiveness.

As technological innovations such as cloud computing, the Internet of Things, robotic process automation, and predictive analytics are integrated into organizations, it makes them increasingly susceptible to cyber threats. Fortune 1000 companies, for example, have a 25% probability of being breached, and 10% of them will face multi-million loss. In smaller companies, 60% will be out of business within six months of a severe cyberattack. This means that governing and assessing cyber risks becomes a prerequisite for successful business performance — and that investors need to know how vulnerable companies really are.

This need for transparency has been recognized by the regulators and facilitated by the new cyber security rules. Currently, the U.S. Security and Exchange Commission (SEC) has increased its enforcement to ensure companies maintain adequate cybersecurity controls and appropriately disclose cyber-related risks and incidents.

BA, Boots and BBC staff details targeted in Russia-linked cyber-attack

The Guardian: Hack attributed to criminal gang hit MOVEit software used by third-party payroll provider Zellis

British Airways, Boots and the BBC are investigating the potential theft of personal details of staff after the companies were hit by a cyber-attack attributed to a Russia-linked criminal gang.

BA confirmed it was one of the companies affected by the hack, which targeted software called MOVEit used by Zellis, a payroll provider.

"We have been informed that we are one of the companies impacted by Zellis's cybersecurity incident, which occurred via one of their third-party suppliers called MOVEit," said a spokesperson for the airline.

An email sent to BA staff told employees that compromised information included names, addresses, national insurance numbers and banking details, according to the Daily Telegraph, which first reported the breach. BA said the hack had affected staff paid through BA payroll in the UK and Ireland.

Payments

Two-thirds of all online shopping scams now start on Facebook and Instagram

Lloyds Banking Group:

- Social media platforms fuelling surge in online shopping scams
- Someone falls victim on Meta-owned platforms every seven minutes
- Estimated £27m being lost by UK consumers each year
- Lloyds Banking Group calls for technology companies to act

Purchase scams starting on Facebook and Instagram are expected to cost UK consumers more than £27m this year alone, according to new analysis by Lloyds Banking Group.

The rising popularity of online shopping has been accompanied by a surge in criminals tricking people into paying for goods and services that don't exist. Victims are lured in by the promise of cut-price or hard-to-find items, often advertised via social media.

They are asked to send money directly from their account to another account via bank transfer (also known as a Faster Payment), which provides very little consumer protection when something goes wrong.

New research by Lloyds Banking Group, based on analysis of reported cases among their more than 25 million retail customers, has found that two-thirds (68%) of all purchase scams now start on just two Meta-owned social media platforms – Facebook (including Facebook Marketplace) and Instagram. This accounts for around 40% the total amount lost to this type of scam.

Google fattens its Wallet to counter Apple Pay

Note: Accessing this article requires a subscription.

American Banker: A year after resurrecting its Wallet product, Google is stacking the app with services to make it a central location for a wide range of consumer transactions and activities.

The company on Thursday made several updates to Google Wallet, focusing on health care and travel services, with potential use cases such as personal identification, airline boarding and other activities. The upgrades come as rival Apple has used Apple Pay and its own wallet to promote cross-selling within Apple's universe by offering consumers a hub for their virtual payments cards along with authentication services.

"There are a lot of different places to store these experiences," said Dong Min Kim, director of product management at Google Wallet. "We want to create one space."

Four Visions For The Future Of Digital Money

Oliver Wyman: Money is about to undergo fundamental changes in the way it is created and used, potentially reordering the financial system.

Executive Summary
Money is about to undergo fundamental changes in the way it is created and used, potentially unleashing a dramatic reordering of the financial system. While volatility has shaken cryptocurrency markets over the past year and caused a string of failures, many parts of the digital asset ecosystem continue to advance largely unaffected by the turmoil, as we explored in an earlier paper.

These include the areas with the greatest long-term potential to transform finance, including the tokenization of financial assets and deposits and the development of central bank digital currencies (CBDCs) by most of the world's largest economies.

The rise of digital assets and distributed ledger technology (DLT) continues to have the potential to upend the competitive landscape, creating new, efficient, nimble competitors, but also offering incumbents a potential new lease on life. Executives and policymakers need to stay focused on the opportunities and risks associated with digital assets.

The future of digital assets as a whole depends heavily on the future of digital money, as payments power the financial system. However, digital money could evolve in quite different ways; for example, there are different forms of digital money that could form the basis of new approaches, spanning CBDCs, tokenized deposits and different types of stablecoins. Executives and policymakers must think in terms of multiple scenarios rather than relying on a single prediction. These approaches will transform business models as they favor different types of issuers and their adoption will reshape liquidity, market-making, and risk management, which could impact the broader financial system considerably.

Quantum

NIST Releases Draft Post-Quantum Encryption Document

Nextgov: The agency continues its post-quantum cryptography push as it looks to create guidance for all sectors.

The latest step in post-quantum cryptography guidance is helping organizations identify where current public-key algorithms will need to be replaced, as the National Institute of Standards and Technology continues its push to fortify U.S. digital networks ahead of the maturity of quantum computing.

A new draft document previews—and solicits public commentary on—NIST's current post-quantum cryptography guidance.

Current goals outlined in the working draft include helping entities locate where and how public key algorithms are utilized in encryption schemes, developing a strategy to migrate these algorithms to quantum-resilient substitutes and performing interoperability and performance testing.

"Organizations are often unaware of the breadth and scope of application and functional dependencies on public-key cryptography within their products, services and operational environments," the draft document reads.

Regulatory

NY Banking Watchdog Says It's About 600 Workers Shy of 'Ideal' Staffing Level

Corporate Counsel: Superintendent Adrienne Harris said DFS continues to review compensation of its regulators, as its staff is paid 30% to 50% less than federal counterparts.

New York's top financial regulator tasked with overseeing the banking and insurance industries and their compliance with state laws continues to speak about the agency's staffing shortages.

A spokesman for the Department of Financial Services said on June 1 it presently has more than 1,200 employees, while the executive budget recommends a workforce of 1,391 fulltime equivalent workers.

DFS Superintendent Adrienne Harris has said a workforce in excess of 1,800 would be ideal for the agency, which took possession of Signature Bank, appointing the Federal Deposit Insurance Corporation as its receiver on March 12.

During a recent Senate public hearing about Signature Bank, Harris told lawmakers she was grateful to them for fully funding DFS for the first time in its history soon after Harris was confirmed into the post in January 2022. prime numbers, no one has yet discovered an efficient way for a classical computer to perform the calculation in reverse.

Technology

Why banks need to start planning to use quantum computing

Note: Accessing this article requires a subscription.

American Banker: Quantum computers will enable banks to improve their loan underwriting models, more accurately calculate loan prepayment and default risks and process more data inputs in their marketing models, according to a blog post published in May 2023 by the American Bankers Association.

Quantum computers will eventually present the threat of breaking the encryption algorithms that banks and credit unions use today. But that is a mitigatable threat, and banks have plenty of uses for quantum computers that have driven the world's largest institutions to invest in the technology.

These quantum computing uses are purely hypothetical at the moment, according to one expert, who said no quantum computer today can solve any real-world problems faster than a classical computer can. But as testing on the technology continues, small- and medium-size banks can expect a clearer list of the potential ways they can use quantum computing in the future.

So far, that list of potential applications includes risk analysis, investment portfolio construction and financial crime monitoring, and it may grow over time.

Quantum Untangled - How to make money from quantum computing in 2023

Note: Accessing this article requires a subscription.

Tech Monitor: Commercialisation begins in the cloud

The average time it takes for a new innovation to become a widespread technology is 39 years. That number comes from a 2015 review of dozens of innovations and their path to commercialisation — everything from lithium ion batteries – a speedy 19 years to widespread market penetration – through to cars, which took a 70 years for the planet to get truly comfortable with.

Quantum computing is older than me - *just*. I was born in 1981, soon after CERN made its first proton-antiproton beam collision. Actually building a working prototype of a quantum computer took almost two more decades, with the first functional quantum computer coming online in 1998 and the first example of quantum commercialisation coming from D-Wave in 2011.

Now, of course, there are entire conferences dedicated to the commercialisation of quantum technologies. The biggest companies and earlier players in the space are also claiming “commercial advantage” is on the horizon. IBM promises quantum advantage by 2026 and a number of investment funds and venture capital firms are now dedicated to the quantum space. But how do you actually make money from such a nascent technology?

Other DXC BCM News

Join us: Banking Transformation Summit 2023 — London, 22nd June

The Banking Transformation Summit 2023 is set to be another fantastic event, and we look forward to seeing you in London on the 22nd of June. Keynote speakers Andy Haigh, DXC's Head of Banking and Capital Markets, and Khal Mohammed, Senior Director of Research at DXC, will talk about the future of banking in a data-rich world. *We encourage our suitable UKI and wider Europe-based customers and prospects to attend!*

Five steps for a Zero Trust-based approach to security in financial services – article in International Banker and Finextra

Cybercrimes in the financial services industry are increasing exponentially. How can organizations keep up and stay safe? Read our latest paper to learn how financial services companies can embrace a Zero Trust-based approach to security: https://lnkd.in/e5xGBhs2. This completes the successful publication of the four key papers for FY23 on banking and capital markets.. Read the related articles on International Banker and Finextra.

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/banking

Subscribe to this report at:
https://connect.dxc.technology/DXC-BCM-News.html

Disclaimer

All statements in this communication that do not directly and exclusively relate to historical facts constitute "forward-looking statements." These statements represent current expectations and beliefs, and no assurance can be given that any goal, plan, or result set forth in any forward-looking statement can or will be achieved, and readers are cautioned not to place undue reliance on such statements which speak only as of the date they are made. Such statements are subject to numerous assumptions, risks, uncertainties, and other factors that could cause actual results to differ materially from those described in such statements, many of which are outside of our control. For a written description of these factors, see the section titled "Risk Factors" in DXC's Annual Report on Form 10-K for the fiscal year ended 31 March 2023, and any updating information in subsequent SEC filings. We do not undertake any obligation to update or release any revisions to any forward-looking statement or to report any events or circumstances after the date of this press release or to reflect the occurrence of unanticipated events except as required by law.

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**.