DXC TECHNOLOGY

Banking and Capital Markets bi-weekly news round-up

5 May 2023
Edition no: 288

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)

'The Godfather of A.I.' just quit Google and says he regrets his life's work because it can be hard to stop 'bad actors from using it for bad things'

Note: Accessing the article requires a subscription

Fortune: Geoffrey Hinton is the tech pioneer behind some of the key developments in artificial intelligence powering tools like ChatGPT that millions of people are using today. But the 75-year-old trailblazer says he regrets the work he has devoted his life to because of how A.I. could be misused.

"It is hard to see how you can prevent the bad actors from using it for bad things," Hinton told *the New York Times* in an interview published [on the 1st of May]. "I console myself with the normal excuse: If I hadn't done it, somebody else would have."

Hinton, often referred to as "the Godfather of A.I.," spent years in academia before joining Google in 2013 when it bought his company for $44 million. He told *the Times* Google has been a "proper steward" for how A.I. tech should be deployed and that the tech giant has acted responsibly for its part. But he left the company in May so that he can speak freely about "the dangers of A.I."

According to Hinton, one of his main concerns is how easy access to A.I. text- and image-generation tools could lead to more fake or fraudulent content being created, and how the average person would "not be able to know what is true anymore."

Concerns surrounding the improper use of A.I. have already become a reality. Fake images of Pope Francis in a white puffer jacket made the rounds online a few weeks ago, and deepfake visuals showing China invading Taiwan and banks failing under President Joe Biden if he is reelected were published by the Republican National Committee at the end of April.

"The Main Resource is the Human"

Note: Accessing the report requires a download

Center for Security and Emerging Technology: A Survey of AI Researchers on the Importance of Compute

Progress in artificial intelligence (AI) depends on talented researchers, well-designed algorithms, quality datasets, and powerful hardware. The relative importance of these factors is often debated, with many recent "notable" models requiring massive expenditures of advanced hardware. But how important is computational power for AI progress in general? This data brief explores the results of a survey of more than 400 AI researchers to evaluate the importance and distribution of computational needs.

Bank Sector

Recent banking crises are rooted in a system that rewards excessive risk-taking – as First Republic's failure shows

Note: Accessing the article requires a subscription

The Conversation: First Republic Bank became the second-biggest bank failure in U.S. history after the lender was seized by the Federal Deposit Insurance Corp. and sold to JPMorgan Chase on May 1, 2023.

First Republic is the latest victim of the panic that has roiled small and midsize banks since the failure of Silicon Valley Bank in March 2023.

The collapse of SVB and now First Republic underscores how the impact of risky decisions at one bank can quickly spread into the broader financial system. It should also provide the impetus for policymakers and regulators to address a systemic problem that has plagued the banking industry from the savings and loan crisis of the 1980s to the financial crisis of 2008 to the recent turmoil following SVB's demise: incentive structures that encourage excessive risk-taking.

BigTech

Apple's New Savings Account Draws Nearly $1 Billion In Deposits In First Four Days

Note: Accessing the article requires a subscription

Forbes: Apple's freshly launched high yield savings account brought in as much as $990 million in deposits over its first four days, according to two sources familiar with the matter. On launch day alone, the savings account drew nearly $400 million deposits.

The account's eye-catching 4.15% annual return, plus the ubiquity of iPhones, is likely the main driver for account openings, especially when the average bank is paying less than half a percent. By the end of launch week, roughly 240,000 accounts had been opened, one source adds. The account is offered through a partnership with Goldman Sachs Bank USA. Goldman's own high yield savings account housed under its consumer brand, Marcus, offers a 3.90% return, notably less than the Apple product. When asked about the deposit and account figures, Apple and Goldman Sachs declined to comment.

"Banks have quickly responded to the Fed's interest rate hikes with higher mortgage and car loan rates, but savers have seen little to no increase in traditional bank deposits or savings accounts," Richard Crone, CEO and founder of payments firm Crone Consulting, says. "There's an outflow to CDs, money market funds, and fintechs like Apple."

DXC's Perspective

Apple was able to draw in almost $1bn of deposits to its new savings account in just four days. The 'too-good-to-refuse' interest rate of 4.15% would suggest that brand, customer loyalty and digital experience only count for so much in the battle for market share. The strongest force in banking remains customer inertia.

David Rimmer
Technology Strategy Consultant
DXC Technology

Cloud

Alibaba makes play for Chinese cloud market with aggressive price cuts

National Technology News: Chinese tech and e-commerce giant Alibaba has announced aggressive price cuts for products and services from its cloud computing division as it looks to seize a larger market share of the country's cloud market.

The company [on the 26th of April] revealed price cuts of up to 50 per cent in cloud services. Prices for elastic computing services which use Arm and Intel-based chips have decreased by 15-20 per cent, while services using Nvidia's V1000 and T4 graphics processing units have dropped by between 41-47 per cent.

Alibaba was one of the first entrants into China's cloud computing market, and currently has a share of more than a third of the market. The company however has in recent years faced intensifying competition from other domestic players such as China Telecom and China Unicorn.

This is the first major announcement from Alibaba Cloud since the overall group's split in March. In the biggest restructure in its history, Alibaba in March announced plans to split into six business groups, each with their own chief executive officer and board of directors and the ability to raise outside funding.

Cloud customers should consider options following Ofcom report

Pinsent Masons: Cloud customers will want to consider their options following the recent publication by Ofcom of its interim report into the cloud infrastructure services market.

The 220-page report published in accordance with Ofcom's market study powers under the Enterprise Act 2002 highlighted practices which the regulator considers potentially hinder and restrict competition; in particular a customer's ability to switch provider and adopt a multi-cloud architecture. It is proposing to refer the market for an in-depth investigation by the Competition and Markets Authority (CMA).

Ofcom's concerns focus on three practices:

- data egress fees, which are fees which suppliers charge customers to transfer data out of the cloud to another provider and, in some cases, move services within their own cloud environment;
- technical restrictions which hinder interoperability and portability; and
- committed spend discounts to encourage customers to switch to the cloud initially and to continue to move further services to the cloud.

The report finds that these practices in combination are particularly influencing larger customers to concentrate all of their cloud infrastructure services in the hands of one cloud provider.

DXC's Perspective

The potential for the cloud services market (IaaS and PaaS) to get referred to the Competition and Markets Authority (CMA) in the UK will no doubt cause some customers to re-examine their overall cloud strategy to ensure they can exit any provider's cloud services and maintain the ability to leverage their buying power in the future. DXC's Cloud Right ™ approach works with customers on their strategic rationale for cloud adoption and helps ensure that workload portability and exit strategy is taken into account as part of any cloud migration approach.

Jay Hibbin
Head of Cloud, EMEA
DXC Technology

Cybersecurity

You don't have to wait for quantum computing to prepare for it

The Register: Rapid7 CSO Jaya Baloo on how to tackle this potential looming tech

AI was all the rage at RSA Conference this year, though there was another tech buzzword that managed to make its presence felt: quantum computing, and the security threat those systems may or may not someday pose.

Jaya Baloo, now CSO at Rapid7 and previously CISO at Avast, gave a talk at RSAC on pragmatic preparation for a possible quantum-powered future, and sat down to talk with us about what organizations can do today.

"This isn't a niche message," Baloo told us, adding it really doesn't matter if we don't know right now what the quantum computers of the future might look like or the algorithms they run. Rather than assuming quantum computers won't ever be a threat, it's safer to assume they might be, and that the data you're collecting, encrypting, and retaining now may already be in a position to be compromised in the future by some powerful machine.

Microsoft is giving hackers weather-themed names like storm, typhoon, and blizzard

The Verge: Microsoft has started naming hackers after the weather in a new naming taxonomy update.

Hackers will now be named after events like storms, typhoons, and blizzards, as part of eight groups that Microsoft is using to track cyber-attacks. That means the Lapsus$ hacking group that has targeted companies like Nvidia, Samsung, and Microsoft will now be referred to as Strawberry Tempest (no, it's not a $15 cocktail).

The new taxonomy will include five key groups: nation-state actors, financially motivated actors, private sector offensive actors (PSOAs), influence operations, and groups still in development. If a new cybersecurity threat is new or from an unknown source, then Microsoft will assign it a temporary "Storm" designation and a four-digit number. This replaces the previous "DEV" moniker Microsoft used to use.

Nation-state hackers will be named after a specific family of weather events, designed to indicate where the groups are being directed from. This includes:

- China - Typhoon
- Iran - Sandstorm
- Lebanon - Rain
- North Korea - Sleet
- Russia - Blizzard
- South Korea - Hail
- Turkey - Dust
- Vietnam - Cyclone

DXC's Perspective

Given the long-lived nature of smart meters, other IoT devices and the timeframe for maturation of quantum computing [*which some argue is shorter than the timeframe for obsolescence of long-lived devices*], there is an increasing buzz in security circles about the need to start planning to implement post quantum cryptographic methods for key exchange, encryption and digital signatures.

In 2022, National Institute of Standards and Technology (NIST) published the Post Quantum Cryptography standards – Kyber for Key Exchange and Public Key Encryption; Dilithium for Digital Signatures. Both these methods use lattice cryptography, which is robust against quantum computer attacks.

Zohair Gangjee
Managing Director
Banking and Capital Markets
DXC Technology

Why organizations should prepare for quantum computing cybersecurity now

EY: Quantum technology is finding its way out of research labs and into commercial applications, upending the norms of cryptography.

In brief

- The current approach to data security is susceptible to ever-growing threats without the inclusion of quantum technology.
- Over the next five years, the technology will be in far greater use, requiring organizations to adapt as they await regulatory clarity.
- Ensure you're asking the right questions to assess your priorities and place on the quantum journey.

Exponentially growing data and computational needs have frequently overwhelmed binary computer systems — yet quantum computing (QC) is beginning to pick apart previously unsolvable problems through a step change in processing power. Fundamentally new computer system architectures, communication networks, software and digital infrastructure are now possible.

However, this technology will also disrupt the cryptography that is central to cybersecurity — thereby intensifying existing risks and giving rise to new threats, especially regarding the resilience of cryptographic algorithms. Because of QC's superior computational power, various cryptographic ciphers may inevitably become obsolete and hackable — and those changes are not far away.

Companies Flummoxed by Regulatory Chaos Around Cybersecurity

Corporate Counsel: "There's a lot of unpredictability right now. There's a lot of head-scratching about what's going to come next—what sectors are going to get hit with the next emergency directive, for example," said Megan Leef Brown, a partner with Wiley Rein.

What You Need to Know

- The American Bar Association hosted a panel on April 27 on the fragmented cybersecurity regime.
- Some companies feel second-guessed instead of supported.
- The newly created White House Office of the National Cyber Director has promised to bring harmony to the landscape.

Companies are facing an increasingly unpredictable, burdensome and fragmented regulatory regime when it comes to cybersecurity. Such was the prevailing message at a virtual panel on cybersecurity law and policy hosted by the American Bar Association's Homeland Security Law Institute.

Megan Leef Brown, a partner with Wiley Rein, said the private sector is struggling to handle multiple reporting obligations regarding data breaches or ransomware attacks. "I'm seeing major shifts in the regulatory landscape, some of which I really find quite troubling. It's daunting for the private sector.

Chinese hackers outnumber FBI cyber staff 50 to 1, bureau director says

CNBC:

KEY POINTS

- U.S. cyber intelligence staff is vastly outnumbered by Chinese hackers, Federal Bureau of Investigation Director Christopher Wray told Congress as he pleaded for more money for the agency.
- Wray said the country has "a bigger hacking program than every other major nation combined and have stolen more of our personal and corporate data than all other nations—big or small—combined."
- The agency is requesting about $63 million to help it beef up its cyber staff with 192 new positions.

U.S. cyber intelligence staff is vastly outnumbered by Chinese hackers, Federal Bureau of Investigation Director Christopher Wray told Congress as he pleaded for more money for the agency.

"To give you a sense of what we're up against, if each one of the FBI's cyber agents and intel analysts focused exclusively on the China threat, Chinese hackers would still outnumber FBI Cyber personnel by at least 50 to 1," Wray said in prepared remarks for a budget hearing before a House Appropriations subcommittee on April 27.

Hackers Are Finding Ways to Evade Latest Cybersecurity Tools

Note: Accessing the article requires a subscription

Bloomberg: EDR software has grown in popularity as a way to defend against destructive attacks such as ransomware. Breaches involving the technology are small but growing, researchers say.

As hacking has gotten more destructive and pervasive, a powerful type of tool from companies including CrowdStrike Holdings Inc. and Microsoft Corp. has become a boon for the cybersecurity industry.

Called endpoint detection and response software, it's designed to spot early signs of malicious activity on laptops, servers and other devices – "endpoints" on a computer network — and block them before intruders can steal data or lock the machines.

But experts say that hackers have developed workarounds for some forms of the technology, allowing them to slip past products that have become the gold standard for protecting critical systems.

For instance, in the past two years, Mandiant, which is part of Alphabet Inc.'s Google Cloud division, has investigated 84 breaches where EDR or other endpoint security software was tampered with or disabled, said Tyler McLellan, a principal threat analyst with the company.

DXC

Five data trends that will define the future of banking

DXC: An article about how data-driven technologies can help traditional banks transform customer experience and automate repeated processes

The recent bank bailouts and buyouts have created an atmosphere of concern and uncertainty in the banking industry. Additionally, traditional banks face significant challenges amid changing consumer behavior, an economic landscape still recovering from the impact of COVID-19 and competition from born-in-the-cloud challenger banks. In this increasingly demanding environment, bankers have the chance to fight back by investing further in their digitalization programs.

AI, data analytics and automation technologies offer an opportunity to transform customer experience and automate repeated processes. With these tools, banks can supercharge their operations by delivering relevant data and insights at the right time and speed to the right people, optimizing and accelerating decision making.

At the heart of this transformation is data. Properly sourcing, managing, interpreting and protecting data will be the key ingredient for banks to grow, manage risk and make strategic investments for years to come.

FinTech

The Future of Money, Finance and Banking

Rise by Barclays: An innovation thesis, the first of its kind published by Barclays

This Innovation Thesis explores the seismic shift financial services is facing and the driving forces behind it, and highlights the themes we consider will prove most relevant in the coming years:

- The Future of Money: Payments 2.0, Digital Money and Beyond
- The Future of Finance: Personalised and Embedded
- The Future of Banking: Harnessing technology to build the bank of the future

The Innovation Thesis has been developed by the Barclays FinTech Venture Studio powered by Rainmaking. Our mission is to ideate, prototype quickly and support to scale innovative new products and services. We do this through collaborations with FinTechs, internal teams and corporate clients.

Payments

Visa CEO downplays the threat of FedNow

Note: Accessing the article requires a subscription

American Banker: Visa's chief executive insists that the Federal Reserve's instant settlement system's impending launch should not hurt the card network's own real-time payment options.

- FedNow is expected to launch in July, joining The Clearing House's RTP network in the U.S. as an option for instant settlement. Both systems have the potential to compete with Visa Direct, which uses Visa's debit rails to enable real-time transfers between cardholders. Visa Direct is used by 66 ACH networks, 11 real-time payment networks and 16 card-based networks with the potential to reach more than 7 billion endpoints globally, according to the card network.

- "The most instructive thing to do is look around the world. The U.K. has had Faster Payments [the U.K.'s real-time system] for 15 years and we haven't seen much if any impact on our U.K. debit volume," said Ryan McInerney, Visa's CEO, during the earnings call. "And the U.K. is a growing market for Visa Direct."

Regulatory

The NYSDFS Report on the Failure of Signature Bank

Note: Accessing the article requires a subscription

Bank Reg Blog: Further details on Signature's data and projections that regulators found unreliable

I admit that in the deluge of Federal Reserve Board/FDIC/GAO reports late last week I had missed until Sunday afternoon that the New York state financial regulator had on Friday released its own review of Signature Bank's failure.

In general, the DFS report paints the same broad outline of events at Signature as does the FDIC's report, but there are a few details that I cannot recall reading elsewhere. There are also a few recommendations in the DFS report that could have implications for still-existing banks with a New York charter.

Further details on what sparked the DFS crisis of confidence in Signature's leadership

The DFS has said that the closure of Signature Bank occurred after the bank had "failed to provide reliable and consistent data, thus creating a crisis of confidence in the bank's leadership." On Friday the 28th we talked about one example of these failures included in the FDIC report.

Other DXC BCM News

Join us: AWS Summit, London, 7th June

Please join us and invite customers to meet us at the DXC booth, where we will showcase the game-changing power of technology that we're delivering with AWS, from app and mainframe modernisation to DXC SPARK IoT. DXC is proud to be a Gold Sponsor at the AWS Summit. **LEARN MORE & REGISTER**.

"Data Fabric Approach to Financial Compliance" — blog

This blog piece, prepared in association with BlackSwan Technologies, explains how a data fabric approach can help firms with aspects of financial compliance such as: know your customer (KYC), transaction monitoring, screening and more. **READ MORE**.

Celebrating Earth Day: Walking/Racing and Planting Trees

Our EMEA Banking & Capital Markets and UKI Commercial teams celebrated Earth Day in April by virtually racing around the world in an Earth Day Walk. Over 70 teams and 350 participants logged their steps in an attempt to walk 40,000km — and also planted 400 trees through the Earth Day Canopy Project. **READ MORE**.

"Why building societies should embrace Embedded Finance" — blog

Maintaining relevance to younger customers is a key consideration for building societies, and one method for staying relevant could be using embedded finance solutions — to expand service offerings beyond the sector's focus on savings and mortgages. In a guest blog for the Building Societies Association (BSA), Dhritiman Mukherjee and Guy Griffin, both with DXC, introduce embedded finance: what it is, its benefits and relevance to the building society sector, and details of a typical proposition. **READ MORE**.

Join us: Security Transformation in Financial Services Summit 2023 — London, 26th May

The Security Transformation in Financial Services Summit in London is set to be another fantastic event, and we look forward to seeing you there on 26th May. DXC's Head of Global Security, Mark Hughes, will be a keynote speaker and take part in a panel session. *We encourage our suitable UKI and wider Europe-based clients and prospects to attend!* Please feel free to like and share these posts about the event: **LinkedIn** and **Twitter**.

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.

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**.