DXC TECHNOLOGY

# Banking and Capital Markets bi-weekly news round-up

19 May 2023
Edition no: 289

# 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)

## Will A.I. Become the New McKinsey?

**Note: Accessing the article requires a subscription**

**The New Yorker:** As it's currently imagined, the technology promises to concentrate wealth and disempower workers. Is an alternative possible?

When we talk about artificial intelligence, we rely on metaphor, as we always do when dealing with something new and unfamiliar. Metaphors are, by their nature, imperfect, but we still need to choose them carefully, because bad ones can lead us astray.

For example, it's become very common to compare powerful A.I.s to genies in fairy tales. The metaphor is meant to highlight the difficulty of making powerful entities obey your commands; the computer scientist Stuart Russell has cited the parable of King Midas, who demanded that everything he touched turn into gold, to illustrate the dangers of an A.I. doing what you tell it to do instead of what you want it to do.

There are multiple problems with this metaphor, but one of them is that it derives the wrong lessons from the tale to which it refers. The point of the Midas parable is that greed will destroy you, and that the pursuit of wealth will cost you everything that is truly important. If your reading of the parable is that, when you are granted a wish by the gods, you should phrase your wish very, very carefully, then you have missed the point.

## Security Risks of AI

**Crypto-Gram:** Stanford and Georgetown have a new report on the security risks of AI—particularly adversarial machine learning—based on a workshop they held on the topic.

Jim Dempsey, one of the workshop organizers, wrote a blog post on the report: As a first step, our report recommends the inclusion of AI security concerns within the cybersecurity programs of developers and users. The understanding of how to secure AI systems, we concluded, lags far behind their widespread adoption. Many AI products are deployed without institutions fully understanding the security risks they pose.

Organizations building or deploying AI models should incorporate AI concerns into their cybersecurity functions using a risk management framework that addresses security throughout the AI system life cycle. It will be necessary to grapple with the ways in which AI vulnerabilities are different from traditional cybersecurity bugs, but the starting point is to assume that AI security is a subset of cybersecurity and to begin applying vulnerability management practices to AI-based features.

## How AI Knows Things No One Told It

**Note: Accessing the article requires a subscription**

**Scientific American:** Researchers are still struggling to understand how AI models trained to parrot Internet text can perform advanced tasks such as running code, playing games and trying to break up a marriage

No one yet knows how ChatGPT and its artificial intelligence cousins will transform the world, and one reason is that no one really knows what goes on inside them. Some of these systems' abilities go far beyond what they were trained to do—and even their inventors are baffled as to why. A growing number of tests suggest these AI systems develop internal models of the real world, much as our own brain does, though the machines' technique is different.

"Everything we want to do with them in order to make them better or safer or anything like that seems to me like a ridiculous thing to ask ourselves to do if we don't understand how they work," says Ellie Pavlick of Brown University, one of the researchers working to fill that explanatory void.

## The Computer Scientist Peering Inside AI's Black Boxes

**Quanta Magazine:** *Cynthia Rudin wants machine learning models, responsible for increasingly important decisions, to show their work.*

Machine learning models are incredibly powerful tools. They extract deeply hidden patterns in large data sets that our limited human brains can't parse. These complex algorithms, then, need to be incomprehensible "black boxes," because a model that we could crack open and understand would be useless. Right?

That's all wrong, at least according to Cynthia Rudin, who studies interpretable machine learning at Duke University. She's spent much of her career pushing for transparent but still accurate models to replace the black boxes favored by her field.

The stakes are high. These opaque models are becoming more common in situations where their decisions have real consequences, like the decision to biopsy a potential tumor, grant bail or approve a loan application. Today, at least 581 AI models involved in medical decisions have received authorization from the Food and Drug Administration. Nearly 400 of them are aimed at helping radiologists detect abnormalities in medical imaging, like malignant tumors or signs of a stroke.

Many of these algorithms are black boxes — either because they're proprietary or because they're too complicated for a human to understand. "It makes me very nervous," Rudin said. "The whole framework of machine learning just needs be changed when you're working with something higher-stakes."

## Tech giants forced to reveal AI secrets – here's how this could make life better for all

**The Conversation:** The European Commission is forcing 19 tech giants including Amazon, Google, TikTok and YouTube to explain their artificial intelligence (AI) algorithms under the Digital Services Act.

Asking these businesses – platforms and search engines with more than 45 million EU users – for this information is a much-needed step towards making AI more transparent and accountable. This will make life better for everyone.

AI is expected to affect every aspect of our lives – from healthcare, to education, to what we look at and listen to, and even how how well we write. But AI also generates a lot of fear, often revolving around a god-like computer becoming smarter than us, or the risk that a machine tasked with an innocuous task may inadvertently destroy humanity. More pragmatically, people often wonder if AI will make them redundant.

We have been there before: machines and robots have already replaced many factory workers and bank clerks without leading to the end of work. But AI-based productivity gains come with two novel problems: transparency and accountability. And everyone will lose if we don't think seriously about the best way to address these problems.

## I unintentionally created a biased AI algorithm 25 years ago – tech companies are still making the same mistake

**The Conversation:** In 1998, I unintentionally created a racially biased artificial intelligence algorithm. There are lessons in that story that resonate even more strongly today.

The dangers of bias and errors in AI algorithms are now well known. Why, then, has there been a flurry of blunders by tech companies in recent months, especially in the world of AI chatbots and image generators? Initial versions of ChatGPT produced racist output. The DALL-E 2 and Stable Diffusion image generators both showed racial bias in the pictures they created.

My own epiphany as a white male computer scientist occurred while teaching a computer science class in 2021. The class had just viewed a video poem by Joy Buolamwini, AI researcher and artist and the self-described poet of code. Her 2019 video poem "AI, Ain't I a Woman?" is a devastating three-minute exposé of racial and gender biases in automatic face recognition systems – systems developed by tech companies like Google and Microsoft.

The systems often fail on women of color, incorrectly labeling them as male. Some of the failures are particularly egregious: The hair of Black civil rights leader Ida B. Wells is labeled as a "coonskin cap"; another Black woman is labeled as possessing a "walrus mustache."

# Bank Sector

## US banking crisis: Close to 190 banks could collapse, according to study

**Yahoo! Finance:** With the failure of three regional banks since March, and another one teetering on the brink, will America soon see a cascade of bank failures?

Bloomberg reported Wednesday that San Francisco-based PacWest Bancorp is mulling a sale.

Last week, First Republic Bank became the third bank to collapse, the second-largest bank failure in U.S. history after Washington Mutual, which collapsed in 2008 amid the financial crisis.

After the demise of Silicon Valley Bank and Signature Bank in March, a study on the fragility of the U.S. banking system found that 186 more banks are at risk of failure even if only half of their uninsured depositors (uninsured depositors stand to lose a part of their deposits if the bank fails, potentially giving them incentives to run) decide to withdraw their funds.

Uninsured deposits are customer deposits greater than the $250,000 FDIC deposit insurance limit.

# Cloud

## Amazon Prime Video team throws AWS Serverless under a bus

**The Stack:** Amazon Prime Video has dumped its AWS distributed serverless architecture and moved to what it describes as a "monolith" for its video quality analysis team in a move that it said has cut its cloud infrastructure costs 90%.

The shift saw the team swap an eclectic array of distributed microservices handling video/audio stream analysis processes for an architecture with all components running inside a single Amazon ECS task instead.

(Whether this constitutes a "monolith" as it is described in a Prime Video engineering blog that has triggered huge attention its or instead is now one large microservice is an open question; it has saved it a lot of money following the approach Adrian Cockcroft describes as "optimiz[ing] serverless applications by also building services using containers to solve for lower startup latency, long running compute jobs, and predictable high traffic.")

### DXC's Perspective

What is striking about this article is the admission that whilst the serverless architecture was great at getting to market quickly, it was unable to deliver the scale needed and was very costly to operate. The Prime team took a step back and re-architected the system to run as microservices on ECS, which greatly improved the scalability and significantly reduced the cost. The ability to step back and reassess is often hard to do, especially in a situation where you are already committed to a cloud native solution. This shows the power of doing Cloud Right™ and choosing the right approach at the right time to deliver the results required. DXC is helping clients take that step back to assess why their cloud strategy isn't delivering in practice and making the changes that will unlock the benefits of doing Cloud Right™.

**Jay Hibbin**
**Head of Cloud**
**Banking and Capital Markets**
**DXC Technology**

# Cybersecurity

## Simplifying Security for the Hybrid Working World

**DXC.com:** The distributed workforce, ever-evolving cyber threats and the complexity resulting from working with multiple security vendors are all factors that require organizations to rethink their approach to cybersecurity.

Cybersecurity is at an inflection point. The move to remote working and the endpoint vulnerabilities that go with it are a permanent part of the new normal.

There are multiple factors causing organizations to rethink their security strategies. For example, ransomware is now a successful business model for a new breed of smart, deep-pocketed bad actors. Also, it is difficult and costly to find and retain cybersecurity professionals with the expertise to protect enterprise data against a new generation of attacks. In addition, most enterprises use multiple tools and solutions that must be managed by lean, in-house security teams.

**First: Simplify**
The first step in dealing with any overwhelming situation is to make it simpler. Organizations don't need to deal with multiple different vendors and tools, each with different license agreements and upgrade cycles that require integration with each other. Reducing their number should be at the top of your to-do list.

## Automation specialist ABB 'hit by Black Basta ransomware attack'

**Tech Monitor:** Hundreds of devices at the automation specialist are said to be out of action as it battles the effects of the breach.

Global automation giant ABB has reportedly suffered a cyberattack at the hands of notorious ransomware gang Black Basta. The breach is said to have affected hundreds of company devices.

ABB is said to have halted VPN connections with clients to prevent criminals from moving onto other networks. Based in Switzerland, the company is one of the world's leading providers of robotic systems. It employs over 100,000 people and reported revenue of $29.4bn last year.

Its clients span the public and private sectors. "ABB operates more than 40 US-based engineering, manufacturing, research and service facilities with a proven track record serving a diversity of federal agencies including the Department of Defense, such as the US Army Corps of Engineers, and Federal Civilian agencies such as the Departments of Interior, Transportation, Energy, United States Coast Guard, as well as the US Postal Service," the company says.

## Is Your Cybersecurity Strategy Falling Victim to These 6 Common Pitfalls?

**NIST:** NIST research reveals misconceptions that can affect security professionals — and offers solutions.

Here's a pop quiz for cybersecurity pros: Does your security team consider your organization's employees to be your allies or your enemies? Do they think employees are the weakest link in the security chain? Let's put that last one more broadly and bluntly: Does your team assume users are clueless?

Your answers to those questions may vary, but a recent article by National Institute of Standards and Technology (NIST) computer scientist Julie Haney highlights a pervasive problem within the world of computer security: Many security specialists harbor misconceptions about lay users of information technology, and these misconceptions can increase an organization's risk of cybersecurity breaches. These issues include ineffective communications to lay users and inadequately incorporating user feedback on security system usability.

"Cybersecurity specialists are skilled, dedicated professionals who perform a tremendous service in protecting us from cyber threats," Haney said. "But despite having the noblest of intentions, their community's heavy dependence on technology to solve security problems can discourage them from adequately considering the human element, which plays a major role in effective, usable security."

## Ex-Uber CSO gets probation for covering up theft of data on millions of people

**The Register:** Exec begged judge for leniency – and it worked

Joe Sullivan won't serve any serious time behind bars for his role in covering up Uber's 2016 computer security breach and trying to pass off a ransom payment as a bug bounty.

A San Francisco judge on Thursday sentenced the app maker's now-former chief security officer to three years of probation plus 200 hours of community service, despite prosecutors' pleas to throw Sullivan in the cooler.

Late last month federal officials urged the judge to sentence Sullivan to 15 months in prison for covering up the theft of data from Uber's IT systems and lying to watchdogs about the intrusion.

"Corporate leaders are called upon to do the right thing even when it is embarrassing, even when it is bad for the company's bottom line," they said. "Nobody, neither corporations nor the executives who lead them, is above the law."

## Boards Are Having the Wrong Conversations About Cybersecurity

**Note: Accessing the article requires a subscription**

**HBR:** Headlines increasingly highlight the consequences of poor cybersecurity practices. Board members with cybersecurity experience are trying to get their fellow members' attention on it. And board members want to provide oversight, even though they just don't have the right questions to ask. Boards need to discuss their organization's cybersecurity-induced risks and evaluate plans to manage those risks. With the right conversations about keeping the company resilient, they can take the next step to provide adequate cybersecurity oversight.

Boards that struggle with their role in providing oversight for cybersecurity create a security problem for their organizations. Even though boards say cybersecurity is a priority, they have a long way to go to help their organizations become resilient to cyberattacks. And by not focusing on resilience, boards fail their companies.

We surveyed 600 board members about their attitudes and activities around cybersecurity. Our research shows that despite investments of time and money, most directors (65%) still believe their organizations are at risk of a material cyberattack within the next 12 months, and almost half believe they are unprepared to cope with a targeted attack.

## DXC
## Five data trends that will define the future of banking

**Global Banking & Finance Review:** 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.

### DXC's Perspective

There is a real danger that banks fall into the ESG trap, where they incur the downside of ESG compliance but miss the upside of ESG revenue. McKinsey's survey points to nearly 40% of consumers being prepared to receive 20% lower than a traditional savings account, if there are green benefits. As it stands, value for the environment, customers and banks is being left on the table owing to failure by banks to develop new products and to educate customers.

**David Rimmer**
**Technology Strategy Consultant**
**DXC Technology**

# ESG

## Most consumers are willing to pay more for green finance products, but banks can't differentiate them

**Tear Sheet:**

- Consumers are willing to put money where their convictions are when it comes to combatting the climate crisis.
- However, limited understanding of product offerings and inability to differentiate in green financial products may be leading to an intention-action gap.

As the realities of climate change are setting in, customers are becoming interested in products that help combat the climate crisis and financial products are no different. However, recent research by McKinsey shows that although consumers are interested in green financial products, their understanding of different product offerings by different banks is low.

Motivation to make banking greener is about to hit the halfway mark as 40% US consumers report interest in choosing climate-linked financial products such as a green checking or a climate screened index fund. Moreover, consumers are willing to put their money where their convictions are with two in three saying they would assign more than 40% of their savings or monthly credit card spending to a green retail banking product.

These interest levels persist across levels of income, household savings, and geographic location.

# Technology

## Quantum computing could break the internet. This is how

**Financial Times:** The next generation of quantum computers will open a new world of possibilities, but also pose enormous risks to our online security.

For the moment, quantum computers, which exploit the spooky physics of subatomic particles, remain too unstable to perform sophisticated operations for long. IBM's Osprey computer, thought to be the most powerful quantum computer yet developed, only has 433 qubits (or quantum bits) when most computer scientists consider it would take 1mn to realise the technology's potential. That may still be a decade away.

But in 1994 the American mathematician Peter Shor wrote an algorithm that could theoretically run on a powerful quantum computer to crack the RSA encryption protocol most commonly used to secure online transactions. The RSA algorithm exploits the fact that while it is very easy to multiply two large prime numbers, no one has yet discovered an efficient way for a classical computer to perform the calculation in reverse.

# Other DXC BCM News

## 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 President of 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**.

## 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**.

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

The Banking Transformation Summit in London will likely be an excellent event, and we hope to see you there on 22nd June. Andy Haigh, DXC's Head of Banking and Capital Markets, and Khal Mohammed, Senior Director of Research will be keynote speakers, talking about the future of banking in a data-rich world. *We encourage our suitable UKI and wider Europe-based clients and prospects to attend!*

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**.