

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

21 April 2023  
Edition no: 287

# 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.simoese@dxc.com](mailto:jean-paul.simoese@dxc.com)

## Contents

<b>Artificial Intelligence (AI)</b> .....	<b>1</b>
Google chief warns AI could be harmful if deployed wrongly.....	1
The U.S. government would like to know what its A.I. rules should look like ....	1
Measuring trends in Artificial Intelligence .....	2
<b>Bank Sector</b> .....	<b>2</b>
Bank runs at deadliest in digital age, warns Bailey.....	2
<b>Blockchain</b> .....	<b>3</b>
Blockchain set to disrupt trillions of dollars with billions of users! .....	3
<b>Cloud</b> .....	<b>3</b>
Cloud can reduce greenhouse emissions, but don't assume it's automatic .....	3
<b>Cybersecurity</b> .....	<b>4</b>
How Bank Apps Know You're You.....	4
Amid shifting threats, FIs should be mindful of these emerging cybersecurity risks .....	4
Report Predicts \$8 Trillion in Losses From Cyber Threats This Year .....	5
Payments Giant NCR Hit by Ransomware .....	5
The Cybersecurity Challenges Businesses Are Facing in 2023 .....	6
<b>ESG</b> .....	<b>6</b>
BPIinsights: April 8, 2023.....	6
<b>Payments</b> .....	<b>7</b>
How tiny, cheap smart speakers unlocked the rise of digital payments in India .....	7
<b>Regulator</b> .....	<b>7</b>
Reading Between the Lines: Parsing Regulators' Recent Public Remarks .....	7
Ex-CIO must pay £81k over Total Shambles Bank migration .....	8
<b>Resilience</b> .....	<b>8</b>
Tencent said to have demoted and fired tech bosses after brief outages .....	8
<b>Other DXC BCM News</b> .....	<b>9</b>

## Artificial Intelligence (AI)

### **Google chief warns AI could be harmful if deployed wrongly**

**The Guardian:** Sundar Pichai calls for global regulatory framework similar to nuclear treaty amid safety concerns

Google's chief executive has said concerns about artificial intelligence keep him awake at night and that the technology can be "very harmful" if deployed wrongly.

Sundar Pichai also called for a global regulatory framework for AI similar to the treaties used to regulate nuclear arms use, as he warned that the competition to produce advances in the technology could lead to concerns about safety being pushed aside.

In an interview on [CBS's 60 minutes](#) programme, Pichai said the negative side to AI gave him restless nights. "It can be very harmful if deployed wrongly and we don't have all the answers there yet – and the technology is moving fast. So does that keep me up at night? Absolutely," he said.

### **The U.S. government would like to know what its A.I. rules should look like**

**Note:** The article requires a subscription

**Fortune:** Well, how about that—on the same day that China unveiled its strict new rules for artificial intelligence safety, the U.S. government moved forward with its own, more cautious push to keep A.I. accountable.

While Beijing's rules are typically draconian, imposing censorship on both the inputs and outputs of generative A.I. models, the U.S. National Telecommunications and Information Administration (NTIA) has merely launched a request for comment on new rules that might be needed to ensure A.I. systems safely do what their vendors promise.

Here's NTIA administrator Alan Davidson: "Responsible A.I. systems could bring enormous benefits, but only if we address their potential consequences and harms. For these systems to reach their full potential, companies and consumers need to be able to trust them. Our inquiry will inform policies to support A.I. audits, risk and safety assessments, certifications, and other tools that can create earned trust in A.I. systems."

There are some similarities between what the NTIA is tentatively envisioning and what China's Cyberspace Administration just dictated—though the methods seem quite different.

## **Measuring trends in Artificial Intelligence**

**Artificial Intelligence Index (Stanford University):** Welcome to the 2023 AI Index Report

The AI Index is an independent initiative at the Stanford Institute for Human-Centered Artificial Intelligence (HAI), led by the AI Index Steering Committee, an interdisciplinary group of experts from across academia and industry. The annual report tracks, collates, distills, and visualizes data relating to artificial intelligence, enabling decision-makers to take meaningful action to advance AI responsibly and ethically with humans in mind.

The AI Index collaborates with many different organizations to track progress in artificial intelligence. These organizations include: the Center for Security and Emerging Technology at Georgetown University, LinkedIn, NetBase Quid, Lightcast, and McKinsey. The 2023 report also features more self-collected data and original analysis than ever before. This year's report included new analysis on foundation models, including their geopolitics and training costs, the environmental impact of AI systems, K-12 AI education, and public opinion trends in AI. The AI Index also broadened its tracking of global AI legislation from 25 countries in 2022 to 127 in 2023.

## **Bank Sector**

### **Bank runs at deadliest in digital age, warns Bailey**

**Note: The article requires a subscription**

**The Telegraph (UK):** The rise of social media means that bank runs are faster and more dangerous than ever before, Andrew Bailey has warned.

The [Bank of England Governor](#) said that an unmanageable wave of withdrawals can hit lenders more quickly in the digital age as rumour spreads rapidly and funds can be transferred fast online.

Mr Bailey added that governments must be prepared to allow banks to collapse and savers to lose money under the post-financial crisis framework if the rules are to work.

He told the spring meeting of the [International Monetary Fund](#) (IMF): "If people feel that they can't use the resolution then you've got to come back and ask a really fundamental question. We've just spent ten years or more developing this thing, but is it the right thing?"

"Are uninsured deposits going to bear losses or not? And if they're not, then you have to think very hard, well, how are you going to resolve the bank?"

While Mr. Bailey said he was confident that the system put in place after 2009 to wind down banks worked, he added that it had left savers in smaller lenders, which do not have the buffers of their bigger rivals, more vulnerable in a run.

## DXC's Perspective

Citi's recent report entitled *'Money, Tokens, and Games - Blockchain's Next Billion Users and Trillions in Value'* reinforces that 2023-24 will be the year where adoption of distributed ledger technology (DLT) at an enterprise scale will start to take shape. You only have to look at how seriously American, British, EU, and Asian financial services regulators are advocating for digital asset-friendly regulation.

Also, the issuance of a CBDC, which is underpinned by some form of private or public blockchain technology and the world of Web3. This is only just the beginning; mass adoption is 5-6 years away but now is the time to seriously start to build skills and capability in this technology.

**Rajesh Sadhwani**  
Managing Director, Banking and Capital Markets  
DXC Technology

## DXC's Perspective

Gartner has concluded that *"cloud storage over traditional legacy datacenters can cut associated greenhouse gas (GHG) emissions by 70 to 90 percent"*. However, so much depends on how you measure things: Sweating assets will consume more energy in operations but, by removing the need for replacement hardware, it reduces embodied carbon. This calls for a robust model for sustainability decisions that weighs different considerations and provides an audit trail.

**David Rimmer**  
Technology Strategy Consultant  
DXC Technology

## Blockchain

### **Blockchain set to disrupt trillions of dollars with billions of users!**

**Rich Turrin:** *Blockchain's next billion users and \$9 trillion in disruption is coming sooner than you think!*

Citi's report on blockchain makes it clear that the technology is a "disruptive innovation" poised to transform our world in a big way.

Citi makes an excellent point: "Blockchain is a back-end infrastructure technology without a prominent consumer interface, making it harder to visibly see how it could be innovative."

So unlike cars or the electric light, blockchain won't be visible to users even though it will be behind the metaverse, tokenized assets, and many other products that will become the norm.

#### **-Citi goes all in for blockchain:**

"We believe we are approaching an inflection point, where the promised potential of blockchain will be realized and be measured in billions of users and trillions of dollars in value. Successful adoption will be when blockchain has a billion-plus users who do not even realize they are using the technology."

## Cloud

### **Cloud can reduce greenhouse emissions, but don't assume it's automatic**

**Note:** *The article requires a subscription*

**The Register:** *Organizations can't outsource environmental challenges, warns Gartner*

In a report published in March 2023 titled "Quick Answer: How Green Are Public Cloud Providers?" Gartner concluded that opting for cloud storage over traditional legacy datacenters can cut associated greenhouse gas (GHG) emissions by 70 to 90 percent.

However, the GHG savings that come from adopting cloud do not accrue automatically. The power sources available to your organization, and to hyperscalers, can shift the dial.

"In regions where coal and fossil fuels are key to power generation, datacenters will have the greatest opportunity to reduce GHG emissions by migrating to the cloud. This is because these areas have more CO<sub>2</sub> emitted per hour, and thus have the most room for reduction," said Gartner.

Weather also comes into play by determining how much energy and water is required to keep the infrastructure cool.

"The goal of a public cloud provider is to expend more energy on running the IT equipment than cooling the environment where the equipment resides," the analyst said.

## Cybersecurity

### How Bank Apps Know You're You

**Note: The article requires a subscription**

**The Wall Street Journal:** A lot goes on behind the scenes to keep you safe from hackers

If we've learned one thing from years of hacks and phishing, it's this: A username and a password alone aren't strong enough to protect our most precious accounts.

So why don't our bank apps require us to pile on extra security settings?

Security experts (and our own columnists) have long urged people to turn on two-factor authentication or other tools to secure their apps. Banks, arguably the most sensitive apps on our smartphones, don't often make you use any of that.

Instead, banks run a lot of software in the background to make sure you're really you. Among several factors considered during logins are: the time of day, location, device IP address, mobile carrier, and if any links prompted users to open the app. If anything differs from your unique "fingerprint," your bank might suspect a hacker or a phishing attempt, and prompt you to take more steps to verify your identity.

### Amid shifting threats, FIs should be mindful of these emerging cybersecurity risks

**Tearsheet:**

- The US region was the most heavily targeted for fraudulent card transactions over the period of June 2022 to November 2022.
- A new Visa report highlights several key factors and contributors that elevate risk and fuel vulnerabilities making it possible for bad actors to carry out cyber-attacks and fraudulent activities in current times.

Fluctuating economic headwinds and mobile banking expediting faster payments have created a hotbed for fraudsters to thrive in 2023.

The US region was the most heavily targeted for fraudulent card transactions from both the acquiring bank on the merchant end of the transaction (63.5%) as well as the issuing bank of the cardholder or consumer's bank (38.8%) over the period of June 2022 to November 2022. This indicates that there is a significant gap in security protocols and infrastructure in place to prevent fraudsters from predicting payment credentials, a new [Biannual Threats Report](#) by Visa shows.

As new technologies are enabling commerce to return in new digital and physical formats, fraudsters are continuing to adapt their tactics to find new ways to scam consumers and businesses. This is due to a couple of factors: for instance, the rise of digital payments has transformed money movement, making it easier and faster.

## **Report Predicts \$8 Trillion in Losses From Cyber Threats This Year**

**Note:** The article requires a subscription

**Corporate Counsel:** "Phishing has evolved past the Nigerian prince who wants to give you an inheritance you have never heard of, to somebody that you work with in accounting sending you what looks like a legitimate email saying, 'There has been a last-minute change on the deal, and we need to change the wire transfer numbers,'" said Edward McNicholas, a Ropes & Gray partner.

Mimecast, an email security company, released its [2023 State of Email Security](#) (SOES) report detailing the risks faced by businesses in the form of email-borne attacks and the need to increase the response due to the growing sophistication of those attacks.

The SOES report was compiled by interviewing 1,700 information technology and cybersecurity professionals on the type and volume of attacks experienced and the security measures businesses currently have in place. The report's biggest takeaways included that cyber threats stand to result in \$8 trillion of losses worldwide this year, with 33 billion records stolen.

According to the report, the average cost of a data breach worldwide is \$4.35 million, but more than double that in the United States at \$9.44 million.

"The growing complexity of attacks is leading to a sense of foreboding on the part of the CISOs and other cybersecurity professionals who took part in the SOES survey," the report said. "Three out of four (76%) expect an email-borne attack will have serious consequences for their organization in the coming year. Of these, 7% believe that such an attack is 'inevitable,' while another three out of 10 consider it 'extremely likely.'"

## **Payments Giant NCR Hit by Ransomware**

**Security Week:** US payments giant NCR has confirmed being targeted in a ransomware attack for which the BlackCat/Alphv group has taken credit.

NCR first reported investigating an "issue" related to its Aloha restaurant point-of-sale (PoS) product on April 12. On April 15, the company said a limited number of ancillary Aloha applications for a subset of its hospitality customers had been impacted by an outage at a single data center.

"On April 13, we confirmed that the outage was the result of a ransomware incident. Immediately upon discovering this development we began contacting customers, engaged third-party cybersecurity experts and launched an investigation. Law enforcement has also been notified," [NCR said](#).

The company has been working to restore affected services, but said that impacted restaurants should still be able to serve customers, with only specific functionality being impacted.



## DXC's Perspective

One top challenge within Bitdefender's 2023 Cybersecurity assessment report is the '*extension of cybersecurity capabilities across environments.*' The existing security paradigm of the castle and moat is one in which we created a binary distinction – outside is bad and untrusted; inside is good and trusted. As your castle walls extend into the cloud(s), that paradigm does not contemplate an insider threat. When your attacker is 'on network', it does not matter how high your castle walls are!

**Zohair Gangjee**  
Managing Director, Banking and Capital Markets  
DXC Technology

## The Cybersecurity Challenges Businesses Are Facing in 2023

**Note: The article requires a subscription**

**Bitdefender:** The challenges faced by cybersecurity teams are constantly changing.

Not only are teams having to deal with an increase in ransomware, phishing, and supply-chain attacks, but they are also forced to contend with increasingly complex environments as organizations increase their reliance on hybrid cloud, software supply chain, and SaaS apps.

This environmental complexity overwhelms cybersecurity departments that are already struggling to find the right resources. For some, the current economic crisis has led to minimized budgets and hiring challenges, while others are overburdened with too many vendors, tools, and data sources. As a result, more than half of organizations have suffered a data breach in the past 12 months — and the majority have been asked to keep the data leak under wraps, despite the potential consequences they could face.

Bitdefender [surveyed 400 IT and security professionals](#) globally, ranging from IT managers to CISOs, in various industry sectors working in organizations with 1,000+ employees to discover the biggest cybersecurity challenges businesses face in 2023.

## ESG

### BPIInsights: April 8, 2023

**BPI: NY Fed Releases Climate Risk Staff Reports.**

The Federal Reserve Bank of New York this week published two staff reports on climate risk. One [report](#) covered climate stress testing, while the [other](#) focused on U.S. banks' exposures to climate transition risks.

The climate stress testing report explored the design of climate stress tests and scenarios used by regulators. The authors highlight the need to consider many transition risks as dynamic policy choices; understand and incorporate feedback loops between climate change and the economy; and explore scenarios where climate risks coincide with other risks.

They contend that more research is required to "identify channels through which plausible scenarios can lead to meaningful short-run impact on credit risks, given typical bank loan maturities", incorporate bank lending responses to climate risks, evaluate climate risk pricing in financial markets and take into account how expectations form around the realizations of climate risks. They also suggest ways to improve climate scenario modeling.

## Payments

### How tiny, cheap smart speakers unlocked the rise of digital payments in India

**Rest of World:** Vegetable carts, flower shops, mom-and-pop stores: Small speakers that read out digital payment receipts are making fintech companies big money.

- Digital payments have taken off in India in a big way, but fintech companies have not been making money from facilitating them. Sound boxes are solving this problem.
- The success of Paytm's device has prompted other companies like BharatPe, PhonePe, and MobiKwik to launch their own versions of the sound box.

Abbas Ali, a vegetable vendor in an upscale neighborhood in New Delhi, started accepting digital payments in 2021. But every time a customer paid online, the 48-year-old, who can neither read nor write, would need to call his son to confirm that the payment had been received.

The customers, often in a rush, would get impatient. Ali would have to spend more time attending to them than he had back when he accepted only cash. Eventually, a fellow vendor suggested he subscribe to a "sound box" — a nifty internet-connected device that reads out payment confirmation messages.

## Regulator

### Reading Between the Lines: Parsing Regulators' Recent Public Remarks

**Note:** The article requires a subscription

#### Fintech Business Weekly

The key takeaway from most analysis of Director Chopra's conversation with Washington Post's Lori Montgomery was his view that P2P payment apps, like Cash App and PayPal, could be viewed as 'systemically important.' But the wide-ranging interview covered a number of other areas worthy of further examination:

- On the Trump-era partial rollback of Dodd-Frank, which increased the size at which banks would be subject to additional regulatory requirements (which passed with bipartisan support): Chopra described the change as a clear "mistake," and said, "there is no question that some of the deregulation in recent history helped to contribute to it, and there are clearly some major changes that will need not just by on the regulations but also on how the regulators supervise some of these firms."

## **Ex-CIO must pay £81k over Total Shambles Bank migration**

**The Register:** Yes, the week-long IT meltdown that sparked a multitude of sarcastic Reg headlines

TSB's chief information officer during the British bank's incredible week-long 2018 meltdown didn't check the key supplier responsible for the migration was prepared to push the button before he assured the board that it was, regulators found yesterday.

The Bank of England's Prudential Regulation Authority (PRA) fined Carlos Abarca £81,000 (\$101,000) after making its decision.

Abarca is the only exec to be singled out in the debacle, although the bank has already coughed up a total of £48.6 million (\$60 million) for the botched platform migration, which is estimated to have cost the company £200 million and [CEO Paul Pester his job](#).

In December, the bank was [fined](#) for failures in operational risk management and governance by both the Financial Conduct Authority (FCA) and the PRA. TSB's IT failings were "widespread and serious," said Mark Steward, FCA exec chief of enforcement, at the time.

## **Resilience**

### **Tencent said to have demoted and fired tech bosses after brief outages**

**The Register:** Think the news has execs at Microsoft 365 or AWS quaking in their boots?

A late March outage of Tencent's two major social platforms, WeChat and QQ, resulted in the firing of managers and directors, thereby proving that the hand of justice at the Chinese tech giant is, well, rather strong.

According to [Chinese media outlet Jiemian News](#), which sits on Beijing's [list](#) of approved media outlets, WeChat and QQ went down for a number of hours on March 29. The outage made functionalities like WeChat voice, WeChat payment, QQ file transfer, QQ mailbox and more unavailable until the fault was repaired "later in the day."

The root cause was a cooling system failure at Guangzhou Telecom Data Center. The news outlet said Tencent's management felt the accident exposed an imperfect disaster recovery and emergency plan and the hidden dangers associated.

To pay for these sins, a senior executive vice president and a vice president were reprimanded, two directors were reportedly knocked down to two out of five stars on their performance review, and two general managers and directors were "demoted and dismissed."

## Other DXC BCM News

### Cloud Right™ in Financial Services Marketing Campaign

Pressured by growing customer expectations and the need to modernize legacy systems, the Banking and Capital Markets industry is at a critical juncture. Many banks are turning to cloud as a catalyst for rapid service delivery and increased agility, and those that execute a well-planned cloud strategy with the right skills in place will have tremendous opportunities to achieve competitive advantages and business success.

[Read our paper to learn how and why.](#)

[Watch the video.](#)

[Like and share on LinkedIn.](#)

### techUK Blog during AI Week 2023

In the digital era, the use of AI in financial services is becoming increasingly prevalent. DXC's Murtuza Yusuf has [written a blog post](#) as part of techUK's AI week, showcasing how DXC's AI solutions can optimize customer banking experiences.

If you're looking to stay ahead of the curve and provide the best possible customer experience in the financial services industry, this is a must-read.

### DXC BCM Video Series

Selected videos from the series of interviews with subject matter experts from DXC's Banking and Capital Markets practice.

- **Financial Services and ESG: rethink your strategy**  
In this video David Rimmer discusses the importance customers are placing on sustainability compliance in their strategy and the targets they are setting. [Watch and share this video.](#)
- **What's the bank of the future when it comes to true data-driven insights?**  
Unstructured data is currently attracting a lot of interest among banking and capital market innovators. What exactly is it, and why is it important? More crucially, what does the bank of the future look like? In this video, Andy Haigh provides his vision. [Watch and share this video.](#)
- **Bring Innovation to The Banking Business with the Top Cloud-Based Technology**  
Cloud computing is nothing new. However, cloud has become so pervasive that it is hard to find a single organization that doesn't have some kind of cloud migration roadmap. By taking the right approach to mainframe modernization, financial services companies can maximize the value of existing investments while building an IT environment that is more agile, cost-effective and built for future innovation. In this video, Jay Hibbin, Cloud Right lead at DXC Technology, speaks about why getting cloud right is crucial for this industry. [Watch and share this video.](#)



DXC Technology Banking and Capital Markets bi-weekly news round-up  
[Subscribe and receive this report in your mailbox every other Friday.](#)

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](https://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](https://dxc.com).

© Copyright 2023 DXC Technology Company. All rights reserved.