DXC TECHNOLOGY

Banking and Capital Markets bi-weekly news round-up

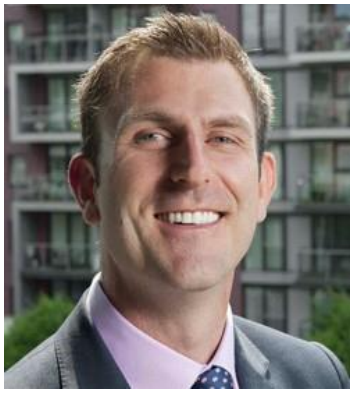
23 June 2023
Edition no: 291

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)

NCSC chief calls for secure AI by design

Pinsent Masons: Businesses developing artificial intelligence (AI) systems must "build in security" to the technology to avoid mistakes made when the internet was developed, the head of the UK's National Cyber Security Centre (NCSC) has said.

In a speech, Lindy Cameron, chief executive of the NCSC, said digital infrastructure relied on was "never designed with security at its heart" and was therefore "built on foundations that are flawed and vulnerable". She said there is a risk that "a similarly flawed ecosystem for AI" could be built unless action is taken now to embed a 'security by design' approach into its development. In doing so, she said, AI developers must "predict possible attacks and identify ways to mitigate them".

Cameron said: "We cannot rely on our ability to retro-fit security into the technology in the years to come nor expect individual users to solely carry the burden of risk. We have to build in security as a core requirement as we develop the technology."

"Like our US counterparts and all of the Five Eyes security alliance, we advocate a 'secure by design' approach where vendors take more responsibility for embedding cybersecurity into their technologies, and their supply chains, from the outset. This will help society and organisations realise the benefits of AI advances but also help to build trust that AI is safe and secure to use," she said.

Using AI for loans and mortgages is big risk, warns EU boss

BBC: Discrimination is a more pressing concern from advancing artificial intelligence than human extinction, says the EU's competition chief.

Margrethe Vestager told the BBC "guardrails" were needed to counter the technology's biggest risks.

She said this was key where AI is being used to help make decisions that can affect someone's livelihood, such as whether they can apply for a mortgage.

The European Parliament approved proposed AI rules.

The MEPs vote in favour of the legislation comes amid warnings over developing the tech - which enables computers to perform tasks typically requiring human intelligence - too quickly. Some experts have warned that AI could lead to the extinction of humanity.

In an exclusive interview with the BBC, Ms Vestager said AI's potential to amplify bias or discrimination, which can be contained in the vast amounts of data sourced from the internet and used to train models and tools, was a more pressing concern.

The economic potential of generative AI: The next productivity frontier

McKinsey Digital: Generative AI is poised to unleash the next wave of productivity. We take a first look at where business value could accrue and the potential impacts on the workforce.

AI has permeated our lives incrementally, through everything from the tech powering our smartphones to autonomous-driving features on cars to the tools retailers use to surprise and delight consumers. As a result, its progress has been almost imperceptible. Clear milestones, such as when AlphaGo, an AI-based program developed by DeepMind, defeated a world champion Go player in 2016, were celebrated but then quickly faded from the public's consciousness.

Generative AI applications such as ChatGPT Copilot, Stable Diffusion, and others have captured the imagination of people around the world in a way AlphaGo did not, thanks to their broad utility—almost anyone can use them to communicate and create—and preternatural ability to have a conversation with a user. The latest generative AI applications can perform a range of routine tasks, such as the reorganization and classification of data. But it is their ability to write text, compose music, and create digital art that has garnered headlines and persuaded consumers and households to experiment on their own. As a result, a broader set of stakeholders are grappling with generative AI's impact on business and society but without much context to help them make sense of it.

UN boss recommends nuclear option for AI regulation

The Register: Proposes global brainbox-bossing body based on the International Atomic Energy Agency's blueprint

United Nations secretary-general António Guterres has called for the formation of a global AI watchdog modelled after the International Atomic Energy Agency (IAEA).

"New technology is moving at warp speeds, and so are the threats that come with it," he said in a briefing. "Alarm bells over the latest form of artificial intelligence – generative AI – are deafening, and they are loudest from the developers who designed it."

"These scientists and experts have called on the world to act, declaring AI an existential threat to humanity on a par with the risk of nuclear war. We must take those warnings seriously."

Guterres expressed his preference for UN member states to create an organization to oversee and regulate the development of AI. The agency would operate similarly to the IAEA, which develops and publishes policies and guidelines promoting the safe use of nuclear energy, whilst monitoring and enforcing safeguards preventing the technology's use for weapons development.

BigTech

CFPB seeks to supervise Big Tech firms under larger participant rule

Note: Accessing this article requires a subscription.

American Banker: Giant nonbank payment companies Apple, Google, PayPal and others face the prospect of being examined and supervised as early as next year by the Consumer Financial Protection Bureau.

This week the CFPB released its spring rulemaking agenda that lists significant rules it plans to issue including one new item: a larger participant rule to examine consumer payment markets. The rule will allow the CFPB to conduct oversight of Big Tech companies and potentially test its authority by specifically determining how companies monetize data that may unfairly impact consumers.

"The CFPB has the authority over these systems but we don't know how the technology companies will push back," said Ed Groshans, senior policy and research analyst at Compass Point Research & Trading. "I don't think any of the large technology companies are going to be pleased, but they are involved in fintech and this is part-and-parcel of being in that land."

Meta has 'duty of care' to tackle fraud says TSB CEO

National Technology News: The chief executive of TSB has called on social media behemoth Meta to clampdown on fraud originating on its platforms.

In an open letter to the company, TSB chief executive officer Robin Bulloch wrote that scams originating from Meta platforms – such as Facebook, Instagram and WhatsApp – account for 80 per cent of the fraud it refunds within its three biggest fraud categories (Purchase, Investment and Impersonation). In particular, TSB estimates that over 70,000 purchase fraud cases took place on Facebook Marketplace in 2022.

The letter also cites industry projections which estimate that without interventions, scams originating on Meta platforms could account for up to £250 million of push payment losses to UK households in 2023.

TSB has called on Meta to make five tech interventions including: the introduction of a secure payment mechanism to eliminate dangerous transactions on Facebook Marketplace; the banning of unregulated UK businesses from using Facebook and Instagram to advertise investments and financial products, including cryptocurrencies; a clear public commitment to investigating and, where confirmed, removing all content flagged as potentially fraudulent within 24 hours; filtering out of fraudulent adverts and social media posts such as those using terms like ‘cash flip’ or ‘crypto offer’; and a feature within WhatsApp that flags unknown numbers and warns users to check they are genuine.

Cybersecurity

Barracuda Urges Replacing — Not Patching — Its Email Security Gateways

Krebson**Security:** It's not often that a zero-day vulnerability causes a network security vendor to urge customers to physically remove and decommission an entire line of affected hardware — as opposed to just applying software updates.

But experts say that is exactly what transpired [on June 6] with Barracuda Networks, as the company struggled to combat a sprawling malware threat which appears to have undermined its email security appliances in such a fundamental way that they can no longer be safely updated with software fixes.

Campbell, Calif. based Barracuda said it hired incident response firm Mandiant on May 18 after receiving reports about unusual traffic originating from its Email Security Gateway (ESG) devices, which are designed to sit at the edge of an organization's network and scan all incoming and outgoing email for malware.

On May 19, Barracuda identified that the malicious traffic was taking advantage of a previously unknown vulnerability in its ESG appliances, and on May 20 the company pushed a patch for the flaw to all affected appliances (CVE-2023-2868).

In its security advisory, Barracuda said the vulnerability existed in the Barracuda software component responsible for screening attachments for malware. More alarmingly, the company said it appears attackers first started exploiting the flaw in October 2022.

DXC Perspective

Barracuda's offer to replace affected ESG appliances at no cost would have been cold comfort to their customers. The 8-month window between flaw exploitation and initial patch is worrying enough, particularly as there has been evidence of data exfiltration. Speculation that the attack has the hallmarks of a nation-state attack rather than a ransomware actor would have compounded those woes. Over the past 10 years there has been a steady transition from black-box security to virtual and SaaS platform. Whilst firmware compromise is nothing new, this incident will give companies who haven't yet started their transition away from physical, pause for thought.

Simon Meredith
Security Lead
DXC Technology

China's cyber now aimed at infrastructure, warns CISA boss

The Register: Resilience against threats needs a boost

China's cyber-ops against the US have shifted from espionage activities to targeting infrastructure and societal disruption, the director of the Cybersecurity and Infrastructure Security Agency (CISA) Jen Easterly told an Aspen Institute event on the 12th of June.

"PRC actors have been in the spotlight for years and years, the key difference here was for PRC actors the focus has been espionage," said [VIDEO] Easterly. Easterly's definition of espionage includes intellectual property theft and "the greatest transfer of intellectual wealth in history."

"But what we are starting to see – and this was captured in the IC's annual threat assessment – was targeting that was less about espionage and more about disruption and destruction," she added.

Payments

Why Apple Pay Later is the tortoise in the buy now/pay later race

Note: Accessing this article requires a subscription.

American Banker: Any fintech players in the buy now/pay later market who feared the entrance of Apple have had little to worry about so far, as the rollout of Apple Pay Later has been very quiet.

Since launching the BNPL service in March, Apple has offered early access to consumers it selects seemingly at random. Apple said it plans a broader rollout in "coming months," but observers hear very little buzz and see no competitive impact yet.

Apple Pay Later offers borrowers loans of $50 to $1,000 to be repaid in four equal payments over six weeks with no interest, with a linked debit card required for repayment. Mastercard Instalments provides the connection to merchants, who will pay Apple a fee when consumers make purchases.

Perhaps the $1,000 limit is why Apple Pay Later didn't merit a mention when Apple unveiled its pricey $3,500 mixed-reality headset this week — a product that many people would need to finance.

The initial low visibility of Apple Pay Later contrasts with BNPL giant Affirm, which continues to advertise on thousands of retail partners' websites, and which in recent weeks signed broad agreements with both Worldpay and Amazon to further its merchant reach.

DXC Perspective

Apple has quite rightly wanted to jump on the BNPL wagon as the market size was valued at $23.22bn in 2022 and projected to be $30.38bn in 2023, with continued YoY growth (as estimated by Fortune Business Insights). Unfortunately, BNPL propositions work when properly promoted and positioned to make the consumer's buying journey frictionless, often as part of the check-out process. Apple have yet to achieve this and rely on payment scheme merchant integrations rather than direct merchant partnerships. Time will tell how they evolve their product to drive higher uptake.

Paul Sweetingham
Global Capability Leader: Banking BPO & CX
DXC Technology

EBA finds that money laundering and terrorist financing risks in payments institutions are not managed effectively

European Banking Authority: The European Banking Authority (EBA) published its Report on money laundering and terrorist financing (ML/TF) risks associated with EU payment institutions. Its findings suggest that ML/TF risks in the sector may not be assessed and managed effectively by institutions and their supervisors.

In 2022, the EBA assessed the scale and nature of ML/TF risk in the payment institutions sector. It considered how payment institutions identify and manage ML/TF risks and what supervisors do to mitigate those risks when considering an application for the authorisation of a payment institution and during the life of a payment institution.

The EBA's findings suggest that generally institutions in the sector do not manage ML/TF risk adequately. AML/CFT internal controls in payment institutions are often insufficient to prevent ML/TF. This is in spite of the high inherent ML/TF risk to which the sector is exposed.

The EBA's findings also suggest that not all competent authorities are currently doing enough to supervise the sector effectively.

Regulatory

FDIC, Fed, OCC finalize guidance for banks' third-party partnerships

Note: Accessing this article requires a subscription.

American Banker: Three federal bank regulators finalized risk management guidance for banks to consider when developing relationships with fintechs and other third parties.

The 68-page, interagency report details how banks should evaluate risks when assessing, negotiating with and monitoring third-party relationships. The Federal Reserve, Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency finalized the guidance, nearly two years following the initial draft's publication.

Banks must implement risk management practices that account for the risks of third party providers, such as consultants, merchant payment processors, cloud computing providers and data aggregators, regulators wrote in the guidance. This means executing appropriate due diligence, creating clear expectations for performance and responsibilities and outlining plans in the case of terminating the agreement.

What's in the bipartisan deal on clawbacks from failed-bank CEOs

Note: Accessing this article requires a subscription.

American Banker: Senate Banking Committee Chair Sherrod Brown, D-Ohio, and ranking member Tim Scott, R-S.C., have reached a deal on legislation that would make it easier for regulators to recoup compensation from executives at failed banks.

The Senate Banking Committee is scheduled to vote on a bipartisan bill that would broaden the Federal Deposit Insurance Corp.'s authority to claw back compensation from executives of failed banks.

The legislation was introduced [last] week after Senate Banking Committee Chair Sherrod Brown, D-Ohio, reached an agreement with ranking member Tim Scott, R-S.C.

It would give the FDIC the ability to claw back compensation received by executives from up to 24 months before a bank's failure. That would include incentive-based, equity-based and performance-based compensation, plus any money the executive made from selling shares of the bank. The clawback provisions would not apply to community banks.

The bill would also increase the maximum penalties that regulators can impose on executives who "recklessly" violate the law.

"It's time for CEOs to face consequences for their actions, just like everyone else," Brown said in a statement.

OCC Report Identifies Key Risks Facing Federal Banking System

Corporate Counsel: The Office of the Comptroller of the Currency (OCC) reported the key issues facing the federal banking system in its *Semiannual Risk Perspective for Spring 2023*.

The OCC reported that the overall strength of the federal banking system is sound. The OCC has closely monitored the condition of the institutions it supervises throughout the market stress this spring and has engaged directly with its banks to ensure they are appropriately managing their risks and restoring confidence in the banking system.

The banking system faced increased volatility due to a liquidity crisis in the first quarter of 2023. Banks are focused on stabilizing liquidity and maintaining confidence in the banking system. Banks should remain diligent and maintain effective risk management practices over critical functions to continue to withstand current and future economic and financial challenges.

Highlights from the report include:

- Liquidity levels have been strengthened in response to the failures of several banks and investment portfolio depreciation. Rising long-term rates caused significant depreciation in investment portfolios, focusing attention on banks' liquidity risk profiles.

- Credit risk remains moderate in aggregate, but signs of stress are increasing, for instance in certain segments of commercial real estate. Overall, credit markets and loan portfolios remain resilient, and problem loan levels remain manageable. The persistent drag from high inflation and rising interest rates, however, is causing credit conditions to deteriorate.

Technology

Central banks successfully test 'quantum resistant' communications channel

Finextra: A secure communication channel designed to protect financial data against future threats from quantum computers has been successfully established by the BIS Innovation Hub Eurosystem Centre, in concert with Banque de France and Deutsche Bundesbank.

The Bank for International Settlements bills quantum computing as one of the most significant cybersecurity threats facing the financial system, potentially exposing all transactions and stored financial data to attack. Experts refer to that risk as "Q Day."

To prepare for a transition towards quantum-resistant encryption, the BIS Innovation Hub Eurosystem's Project Leap is investigating how to update and replace the cryptographic security algorithms that the financial system is critically reliant on.

Other DXC BCM News

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 DXC's latest paper to learn how financial services companies can embrace a Zero Trust-based approach to security: https://lnkd.in/e5xGBhs2. This completes the publication of four key papers for FY23 on banking and capital markets.. Read the related articles on International Banker and Finextra.

Executive Data Series: The banking customer in a data-rich world

In the latest conversation of the Executive Data Series, DXC's Head of Banking and Capital Markets (EMEA) Andy Haigh sits down with Mohammed 'Khal' Khalid to discuss how banks can use data and analytics to transform financial services and improve the customer experience.

Listen to the full conversation (23 mins.) or read the transcript: https://dxc.to/3NlsbXI

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**.