POINT OF VIEW

Major Trends in European Retail Banking for 2024

Squaring the Circle of Cybersecurity, Resilience, and Increased Regulatory Pressure

KEY TRENDS FOR 2024:

- Maintaining resilience in the face of change and cybersecurity threats
- AI grows as a friend and foe
- Systems fit for the data and security challenges of ESG
- Embracing better organizational and leadership models

Although 2023 has been a record year for European retail banks, thanks to historically high-interest rates, it has also underlined the changed world we live in. "Crisis mode" is fast becoming the default setting for the financial sector, and European regulators are imposing tougher liquidity and other resilience demands on the sector in response.

For many established players, the traditional platform that was once the foundation of their business is now in danger of becoming a barrier to future growth and agility. Customers expect frictionless, instant service on whatever platform they choose. For the majority of those customers, that platform is the bank's mobile app—often seen as the bank's primary product. For incumbents and startups alike, these services need to be flexible, resilient, and secured in real-time.

Artificial intelligence (AI) is another technology that, having grown substantially in 2023, will continue to evolve. It represents both a friend to financial services organizations—promising benefits in automation, security, and sales and marketing—and a foe, embraced by bad actors to assist them in cyber attacks.

There is a broader change in what consumers and investors want from their banks. Both groups want financial institutions that take notice of environmental, social, and governance (ESG) concerns and not just the bottom line. Supporting ESG and net zero are now primary strategies for almost all banks. Banks need to meet this challenge and create secure systems that support the transparency required for ESG reporting. ESG data requires solid auditing and reporting tools with the flexibility and agility to change to meet new demands from regulators, investors, and shareholders.

WEF Identifies Cybersecurity as a Serious ESG Issue

Retail and institutional ESG investment continues to grow globally and is likely to hit between $14 trillion and $19 trillion by 2025.

In Europe in particular, momentum in ESG is accelerating as the continent embraces the European Green Deal. In July, the European Commission adopted the European Sustainability Reporting Standards (ESRS) for use by all companies subject to the Corporate Sustainability Reporting Directive (CSRD). These standards cover the full range of environmental, social, and governance issues, including climate change, biodiversity, and human rights.

The World Economic Forum (WEF) identifies cyber risk as the greatest and most immediate risk to sustainability for financial institutions. It further notes that cyber risk needs to be a fundamental part of ESG thinking because of the threat it poses to the asset value of financial institutions, and that data breaches and disruptions to financial networks pose a risk to society as a whole.

ESG requires a fundamental change in how banks operate, and a significant part of this challenge is managing the reporting demand—this represents the "G," governance, component of ESG, which is often overshadowed. This marks a step change from traditional year-end accounting and auditing. Robust reporting requires a whole new set of tools, given more complex supply chains and components sourced from different suppliers.

Ensuring the security and privacy of audit data is crucial to protect against data breaches and maintain the trust of customers and regulators. AI has the potential to help with continual monitoring, classifying, and filing of data, as well as performing repetitive processing tasks, minimizing the potential for human error.

ESG investment is likely to hit between

$14 trillion - $19 trillion

by 2025[1].

[1]Broadridge Distribution Insight: ESG and sustainable investment outlook

"Organizations can benefit greatly by exploring the close connection between cyber and ESG risks. Both areas focus on identifying and managing risks and opportunities, leading to enhanced products and solutions and a better society."

- KPMG Cybersecurity in ESG Report

Dealing with DORA, ISO 20022 in Europe

European banks are still dealing with the impact of the Digital Operational Resilience Act (DORA)— the EU regulation that mandates digital resilience for financial institutions.

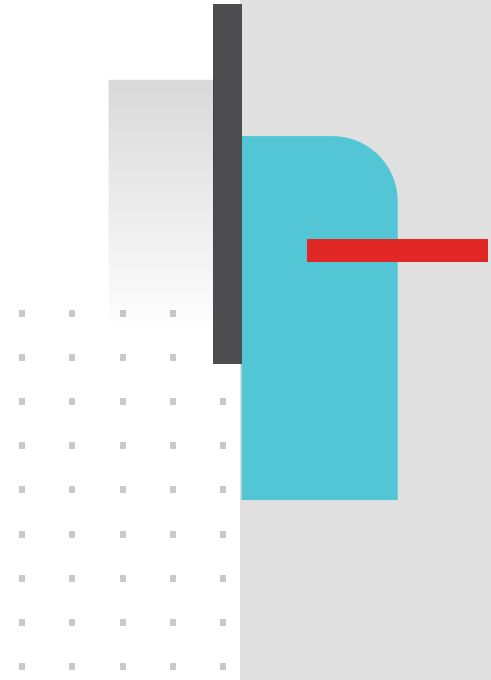
Although full compliance with DORA is not required until January 2025, financial services organizations, defined quite broadly by the new rules, need to be well on their journey by now.

Looking forward, the European Systemic Risk Board sees a growing need or financial institutions to take a more holistic view of security and cyber resilience, testing scenarios and finding ways to measure the impact of incidents or breaches on the wider financial system.

Financial institutions transitioning from SWIFT to ISO 20022—the new international standard for messaging and transactions—need to implement improved cybersecurity to protect the integrity and confidentiality of the richer data being transferred.

Resilience and Liquidity

The European Banking Authority has made clear that it will continue to closely monitor banks' liquidity and national regulator attitudes in light of the bailouts of Credit Suisse and Silicon Valley Bank. The regulator, in its Financial Stability Review, also noted the importance of financial institutions taking cybersecurity seriously: "Accelerated digitalization... comes at a cost of greater exposure to the threat of cyber risks."



Dealing with Risk, Resilience, and Rapid Change

Banks have always been an attractive target for cyber attackers, from criminal gangs to stealthy, state-backed actors. A key trend for 2024 will be building security systems to help banks suffering from "alert overload." This happens when systems are oversensitive and sound frequent alarms for possible fraud or security incidents that need manual checking and intervention from staff. Artificial intelligence (AI) can play a role in reducing the number of incidents that require human intervention.

But broader resilience also requires agility and the ability to respond to changing global conditions. With interest rates and inflation likely to remain high in 2024 and potential deceleration—or worse—in China, financial institutions are facing a year of uncertain outcomes. Global political uncertainty adds to the mix, fueled by conflicts in Europe and the Middle East and the impact of populist and nationalistic politics in many countries. Banks are also seeing outflows from the balance sheets to challenger institutions which are moving from personal accounts to small business accounts and from simple checking accounts to more sophisticated offerings.

Artificial Intelligence and Cybersecurity

Further uncertainty is provided by AI's impact on markets and growing acceptance by consumers, as well as its adoption by Open Banking applications, and by regulators. AI has the potential to transform customer service and communications, risk modeling and compliance reporting, and even contract and loan agreement creation. But it also has major implications for cybersecurity, both positive and negative.

AI is already being used by criminals to find vulnerabilities and to power some attacks, including creating plausible phishing and social interactions.

> "An organization can apply AI in different locations, whether at global research labs or within the organization, and at different stages of the cyber kill chain."
>
> *- Fortinet: Applying Artificial Intelligence to Cybersecurity Beyond the Hype*

But AI is also a powerful defensive tool for detecting and preventing attacks. Solutions like Fortinet's Security Operations platform can bring the power of AI across an organization's security infrastructure providing a joined-up, intelligent system. AI can also help reduce "alert overload" by distinguishing actual threats from false alarms and by automating initial defensive responses. AI is also helping financial institutions to quickly analyze their security logs and other security data to predict future attacks or spot the early stages of network intrusion. This is Fortinet's view of AI-powered security for retail banks.

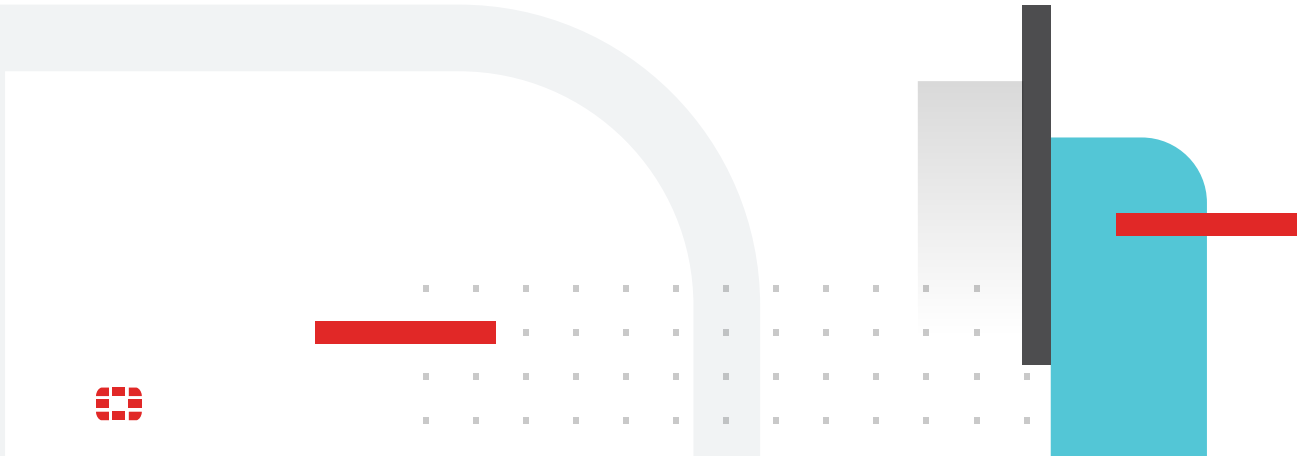
Leadership and Organizational Change

The fundamental challenges faced by European financial institutions are having an impact on people and processes as well as on technology infrastructure. Several analysts share McKinsey's view that the year ahead will see the emergence of new leadership styles and structures to match the new era. Traditional top-down, hierarchical leadership organizational charts are not well-placed to support fast-changing, collaborative, emotionally intelligent decision making.

This requires leadership that moves beyond a focus on profit. It requires a more connected approach to leadership that recognizes the benefit of working with other companies, not just competing with them. Leaders need to listen, learn, empower, and guide as much as they direct, control, and command.

This means a more strategic and central role for the technology leadership too. Banks that have successfully created this change have done so by embracing cloud technology and APIs to turn the bank into a platform at the center of an ecosystem, not just a provider of financial services. CIOs need to evangelize for the positive impact of new technology and how it can allow banks to securely enter brand new markets.

Leaders must also manage the challenges of the hybrid workforce and the changing security risk this brings. Ensuring that all employees have the right up-to-date training will improve your security posture, reduce the risks of serious incidents, and minimize pressure on security help desks.



How Can Technology Help Support These Major Shifts?

Communications

Technology is both an impetus for and a facilitator of these big changes for banks. It is helping to accelerate the digitalization of financial services, from payments to pensions, and is also crucial in mitigating the increased cybersecurity risks that can come from digitization.

Moving to flatter, more networked leadership structures is possible only with better, more secure communication systems. Secure, auditable communications must satisfy both users and regulators while also protecting sensitive information from interception.

Infrastructure and Cloud

Adapting to a landscape of constant change—which McKinsey calls "The Great Banking Transition"— means rethinking how infrastructure is built, maintained, and secured. For most institutions, that means greater use of the cloud, where flexibility and agility are baked in, and responsibility for security is shared.

As banks transition to the cloud, cybersecurity measures are crucial. This is due to the growth of breakthrough technologies in the market, in particular technologies enabling digital representations of value or of rights to be transferred and stored electronically, using distributed ledger or similar technology (crypto-assets), and of services related to those assets.

As data volumes increase exponentially, the potential for cyber fraud, DDOS, and other attacks will need to be mitigated in real time.

Protecting the Legacy

However important the cloud is to future strategy, the reality is that legacy systems and the data they contain still have huge value for most financial institutions and need to be maintained and secured. There are a variety of reasons why organizations choose not to move applications to the cloud. They might be too complex or have a limited lifespan. Or reluctance because of perceived security issues.

Hybrid systems will remain for the foreseeable future. That means ensuring that systems stay safe and that your cloud applications are able to connect securely to extract and use the data they need from your on-premises estate.

Securing the Changes Ahead

The key message from financial institutions in 2023 is that change is accelerating, and that unpredictability is the only certain prediction for the year ahead. That puts cybersecurity at the forefront of institutional strategy.

It's not all change. IT teams continue to strive to do more with less—challenges might be growing but budgets are not. The challenge of finding and keeping the right people with the right skills will also remain. The need for good training and for network, email, and endpoint security remains essential.

But this year also brought some novel ways to defend systems. New tools like AI and machine learning are bringing new insights to security and threat intelligence and changing how organizations can counter the rising tide of attacks.

For more information, visit Fortinet Financial Services Solutions or take our Cyber Threat Assessment.

FORTINET

www.fortinet.com

1847147-1-1-EN