iNFRONT

CeFPro® magazine for non-financial risk professionals

CYBERSECURITY

ESG

FRAUD

RESILIENCE

THIRD PARTY RISK

EXPANDING BEYOND THE TRADITIONAL

Complexities & scale of non-financial risk

INSIDE THIS ISSUE

iNFRONT

CeFPro® magazine for non-financial risk professionals

CONTENTS

Non-Financial Risk Edition

Written by the industry, for the industry

The views and opinions expressed in this publication are those of the thought leader as an individual, and are not attributed to CeFPro or any particular organization.

Gaining clarity in a cloud of uncertainty

Arindam Majumdar
Deputy Chief Risk Officer
Bank OZK

According to the Chinese calendar, 2023 is the Year of the Rabbit, which symbolizes peace and prosperity. This year was predicted to be the "Year of Hope." As we are about to enter the last financial quarter of the year, it's safe to say this year has been anything but a year of peace, stability, and prosperity. To further illustrate the hypothesis, let us glance at the challenges of the recent past, present, and not-too-distant future. The Federal Reserve continues on its hawkish monetary stance as it continues to fight stubborn inflationary conditions while trying to thread the soft landing needle; the US banking sector is still trying to find its footing after the historic bank failures earlier this year; global geopolitical conditions continue to be turbulent as the Russia-Ukraine conflict continues well into its second year with no immediate diplomatic end in sight; the Chinese economy is showing signs of stalling; the 2024 election bandwagon inches closer; artificial intelligence continues its march towards ubiquitous presence in our daily lives and last but not least, global climate patterns seem to suggest that the onset of climate threat is well and truly upon us.

In a turbulent landscape, competition is rarely more prominent; outside of global market changes and geopolitical risks, myriad non-financial risks continue to develop. This issue of the magazine explores the complex nature of non-financial risk. As threat vectors develop, the big conversation (pages 4-5) looks to explore the cybersecurity landscape and challenges balancing compliance.

History has an uncanny way of repeating itself. We recently saw large bank failures in the US and Europe where myopic decision-making, lack of independent internal effective challenge and accountability, and common-sense approach to risk management and strategic planning led to catastrophic events.

Now more than ever, policymakers, risk professionals, and executive leadership teams should prepare to analyze, assess, and plan for the "what-ifs." This approach to scenario-based analysis and decision-making will ensure optimal resilience and insurance strategies, mitigating risks such as concentration as outlined on pages 22-23.

The future is cloudy as usual, but this cloud of uncertainty can be pierced with the clarity of sound decision-making and reasoning from first principles. The diverse nature of this issue provides a backdrop for some best practices and principles, including insight from CeFPro's NFR Leaders report and insights from industry leaders on the upcoming NFR challenges in 'Talking Heads.'

We welcome contributions. If you or your organization are interested in featuring in our next issue, please contact infront@cefpro.com

CONTENT AND AUTHOR SUBMISSIONS
infront@cefpro.com

ADVERTISING & BUSINESS DEVELOPMENT
If you are interested in sponsorship and advertising opportunities, please contact:
sales@cefpro.com

www.cefpro.com

Cyber risk, compliance and quantification

Kishan Majithia
Executive Director, Cyber and Technology Controls
JP Morgan Chase

Ria Thomas
SVP, Head of Cyber Organizational Resilience
Truist

Katherine Cobb
SVP, Cyber Incident Response Manager
Zions Bancorporation

Cyber threats are growing globally, and the financial services industry continues to be a primary target for an attack due to the vast amount of personal data organizations hold. This should motivate the industry to invest in cybersecurity in order to comply with regulations and protect their reputation. The ongoing cybersecurity battle is one that continues to pose new challenges as criminal tactics evolve and regulatory expectations broaden. We sat down with three industry experts in the cyber sector to explore their thoughts on the matter...

What is the correlation between compliance, cyber threats, and the response to those threats?

Katherine: Considering the new 2023 SEC rules, it continues to be a delicate balance. I think the focus should remain on the threat and how you're trying to respond, remediate, contain, and eradicate those threats. There's then an extra burden of knowing what should be reported to law enforcement or regulators and our obligations.

Taking compliance into account, it becomes frustrating thinking about threat actors or cyber attackers. They don't have the red tape and regulations that financial institutions must go through; they just launch an attack. Meanwhile, we're trying to respond to it and stay compliant. However, there's much more to this than simply checking the box.

Ria: Compliance is a business-critical requirement for any company in a highly regulated industry. That being said, regulations – especially cyber regulations - are often an effort by

government entities to protect broader economic and societal interests by seeking to address issues from the types of incidents that have previously wreaked havoc. Businesses, however, need to look at their own tailored threat landscape and assess what measures are needed that go beyond compliance. This approach is key to ensuring their continued growth in a fast-evolving world of cyber threats.

Kishan: It's easy to be compliant but harder to be more resilient to cyber threats, and there's an intersection between those two. Compliance with regulators also means there are some levels of resilience to threats, but a significant portion isn't. Regulations are lagging indicators of things that we already know, for example, attack vectors; we need to be ahead of the curve, especially in certain industries like the military, financial services and pharmaceuticals. I think this makes our job much harder.

How is quantifying cyber risk in dollar terms beneficial and challenging for a financial institution?

Kishan: It's very beneficial to compare cyber risk with other types of risks, certainly in financial services. It's easy to quantify credit and market risks, but it's much harder for cyber risks. The attraction and messaging make it easier if you can quantify it and put risks in dollar terms. However, there's a real challenge in doing that because the industry frameworks, such as Factor Analysis of Information Risk (FAIR), are only as good as our inputs. Often, a level of precision isn't there in terms of specificity. It's a maturing landscape, but it's a massive uphill struggle currently.

As the industry clubs together to work out the broader dimensions, trying to model this might be beneficial, similarly done for other issues across the cyber landscape. There's a real benefit in sharing information and creating broad rules of the road and how you might try different scenarios instead of everyone doing it themselves and coming up short.

Ria: Cyber risk quantification strategies can be immensely helpful in multiple ways. For example, they can help a company assess what realistic insurance coverage may be needed; these quantification strategies may also be crucial during a cyber crisis in helping an executive leadership team to assess critical decisions, such as what to prioritize as the company recovers, or what the implications are if recovery is taking longer than expected.

At the same time, companies often find it challenging to quantify cyber risk because it requires a clear, steely-eyed view of the enormous financial implications of what a potential business disruption - that lasts longer than the standard 72 hours of business continuity planning - may mean. It can also be challenging to quantify certain types of risk, such as reputational risk, that are heightened during a cyber crisis. Yet, it's imperative that companies look at the issue of cyber risk through the lens of quantification.

Katherine: I've not seen this done well yet, and the problem is many variables make it hard to quantify every cyber threat. If somebody clicks on a phishing link, the impact could be zero or massive, depending on what events unfold after that click. How we view organizations after they fall victim to an attack is different, and it depends on two perspectives: Did you have controls, but they failed, or did you not have controls? All of that adds complexity to how the public will view what happened and how it happened.

Which approach is best to take when looking at risk across the board through a cyber lens?

Ria: Often, companies tend to look at cyber purely as a tech risk or, perhaps, a legal or regulatory one. Yet, having advised over two dozen large global firms as they navigated live cyber crises, I've realized that cyber is unique in that it amplifies all the other risks on the risk register.

For example, liquidity or credit risk may not seem to have a direct correlation to a cyber crisis. Yet, in the current environment facing the financial services industry, wherein financial institutions have faced a "run on the bank," a poorly handled cyber crisis can lead to loss of trust and faith, and potentially lead to a circumstance in which other risks – for example, liquidity and credit risks - are amplified.

As such, a critical approach to cyber resilience is to assess what the operational, financial, legal, regulatory and reputational implications of a cyber crisis are when viewed through the lens of all key risks on the risk register. Engaging all relevant stakeholders who own those risks, and ensuring that their broader mitigation efforts are integrated is what provides a holistic approach to cyber resilience.

Kishan: If you're doing them correctly, you see those as risks integrating. Often, a cyber or risk department is siloed, making it hard to explore them properly in a way that resonates with the stakeholders. Understanding the impacts differs from discussing the risk in a way that will lead to something demonstrably different from what we're getting today.

Katherine: I agree with that. When people hear cyber, they immediately think that has nothing to do with them as they don't directly work with cyber. However, if systems go down, all employees are affected; therefore, helping teams see the impact on their area enforces the view that cyber risk isn't just a technology risk. There's definitely not a one-size-fits-all approach.

Cyber risk and security features prominently in CeFPro's Fintech and NFR Leaders survey and reports. For full information on the final reports, and to take part in this year's survey, visit www.cefpro.com/connect to register for a free account.

Sudharshan Narva
Director, Data Analytics Internal Audie
TIAA

The future of fraud detection and prevention

Where do you see the role of machine learning and large language models within a fraud context in the future?
With the rapid growth of Generative AI and machine learning algorithms, businesses are benefiting more than ever. The cycle time from hypothesis to activation has reduced to almost real-time. Since business leaders now have insight at their fingertips, it's created more momentum in adopting AI and machine learning as a tool to detect and prevent fraud.

The role of machine learning and large language models in fraud prevention is poised to become even more crucial. In the immediate term, these technologies can swiftly analyze vast transactional structured and unstructured data streams to identify anomalies and potentially fraudulent activities. This enables real-time detection and mitigation of risks as they emerge.

In the future, machine learning models will be instrumental in adapting to the rapidly changing risk landscape. They can learn from new data patterns and emerging fraud tactics, updating their algorithms to stay one step ahead of fraudsters. From a strategic standpoint, large language models will not only enhance transactional fraud detection but also assist in complex scenarios such as trends, opportunities, root causes, and prescribing the right course of action to detect and prevent fraud systematically. From a risk management perspective, it's crucial to approach these advancements ethically and responsibly. Bias mitigation and transparency will be paramount to ensure fair outcomes and ongoing model validation will be necessary to maintain effectiveness.

How can these technologies be used to protect customers more efficiently?
AI technologies like machine learning, deep learning, and large language models (LLMs) offer a range of ways to enhance customer protection against evolving fraud schemes. The outcomes of these AI applications include reduced false positives, quicker fraud detection, enhanced customer experiences (as legitimate transactions are less likely to be flagged), and, ultimately, a safer financial environment for customers. However, it's important to continually update and refine these models to keep up with the ever-changing market, environmental, socio-economic, and political risks that have a high impact on emerging fraud techniques and ensure that fraudsters do not manipulate the AI itself.

- Detection of sophisticated schemes: AI can identify complex fraud schemes that traditional rule-based systems might miss. For instance, in the case of synthetic identity fraud, where fraudsters create fictitious identities, AI can analyze patterns across vast datasets to detect subtle correlations indicating fraudulent activities.

- Real-time monitoring: Machine learning algorithms can provide real-time monitoring of transactions, flagging suspicious activities as they occur. This is particularly useful for identifying card-not-present fraud, where fraudsters use stolen card details for online purchases.

- Behavioral analysis: AI can build profiles of customer behavior and usage patterns. This enables the system to identify anomalies, such as sudden changes in spending habits, which could indicate account takeover or unauthorized transactions.

- Voice and text analysis: LLMs can be used to analyze voice and text interactions with customers to identify potential fraud. For instance, if a customer's chat interaction suddenly displays signs of distress or coercion, the AI system could trigger a security alert.

- Phishing detection: Deep learning models can be trained to recognize phishing attempts in emails by analyzing sender behavior, message content, and other factors. This helps in preventing customers from falling prey to phishing attacks.

- Application screening: AI-powered systems can quickly analyze loan and credit card applications, cross-referencing information against databases to spot inconsistencies. This detects fraudsters attempting to obtain credit using false information.

- Network analysis: Machine learning can be used to analyze connections between seemingly unrelated accounts. This helps uncover organized fraud networks that collaborate to carry out large-scale scams.

The development of AI technologies is evolving rapidly, with ongoing research focusing on improving model accuracy, interpretability, and adaptability. Additionally, federated learning and differential privacy techniques are being explored to protect sensitive customer data while training effective models.

Do you see the risk of fraudulent acts using AI and machine learning increasing?
Emerging AI technologies can indeed fall into the wrong hands and be exploited by criminals. Here are a few scenarios where AI could be misused, followed by step-by-step controls to curb these frauds:

Scenario 1: AI-powered phishing attacks

- Generation of realistic content: Fraudsters could use AI to generate convincing phishing emails, chats, or messages

that appear legitimate and personalized.
- Targeted attacks: AI could help attackers identify high-value targets based on publicly available information and social media profiles.
- Personalization: AI-generated content could be tailored to imitate specific individuals, making the phishing attempts harder to detect.

Scenario 2: AI-enhanced identity theft
- Synthetic identity creation: Fraudsters could use AI to create synthetic identities by combining real and fake information to pass verification checks.
- Pattern mimicry: AI-powered systems could learn from legitimate behaviors to mimic genuine user patterns, making it harder to detect abnormal activities.
- Biometric manipulation: AI could manipulate biometric data like fingerprints or facial recognition to bypass security measures.

Controls to curb AI-powered fraud:

AI ethics and regulation:
- Enforce ethical guidelines and industry standards to ensure responsible use of AI technologies.
- Regulate AI use in sensitive areas such as finance, healthcare, and identity management.

Advanced authentication:
- Implement multi-factor authentication using a combination of biometrics, one-time passwords, and behavioral analysis.
- Employ liveness detection to prevent the use of manipulated biometric data.

Regular model validation:
- Continuously validate AI models to detect any signs of bias or unfair decision-making.
- Monitor model outputs to identify unexpected or malicious behavior.

AI countermeasures:
- Develop AI-powered solutions to detect AI-generated content. Counter adversarial attacks against AI models.
- Use AI to identify patterns of fraudulent AI usage and adapt to new tactics.

Behavioral analysis:
- Implement AI-driven systems that analyze user behavior for anomalies and deviations from normal patterns.
- Monitor changes in usage, spending habits, and communication style.

Secure data handling:
- Implement robust encryption and data protection mechanisms to prevent unauthorized access to sensitive data.
- Limit access to AI models and datasets to authorized personnel only.

Human oversight:
- Combine AI with human review for critical decisions to ensure a human-in-the-loop approach.
- Human analysts can provide context and intuition that AI may lack.

Public awareness:
- Educate customers about AI-related risks, such as sophisticated phishing attempts, and provide guidance on identifying fraudulent activities.

Collaborative efforts:
- Foster collaboration between tech companies, law enforcement, and regulatory bodies to stay updated on emerging threats and develop effective countermeasures.

What, for you, are some of the key hurdles for fraud teams' successful adoption of technologies such as AI, machine learning, and LLMs?

Addressing these multifaceted hurdles necessitates a holistic approach. It involves mastering the technical intricacies of AI, fostering a supportive organizational culture, enhancing regulatory awareness, and nurturing collaboration between technology and domain experts. The successful evolution of fraud teams requires an orchestrated effort to leverage AI's potential while managing its challenges effectively.

Skill gap and training needs:
A significant hurdle lies in bridging the gap between the existing skill set of fraud teams, and the expertise required to harness AI technologies effectively. Training staff in data science, AI algorithms, and model interpretation is essential for successful integration.

Data complexity and quality:
AI and machine learning thrive on quality data, but fraud detection often involves complex, noisy, and unstructured data. Ensuring data accuracy, completeness, and relevance is a challenge that can impact model performance.

Interpretability vs. complexity:
While AI models offer advanced predictive capabilities, they often lack transparency. Balancing the need for interpretable decision-making with the inherent complexity of some models can be demanding, particularly for regulatory compliance.

Regulatory landscape and compliance:
Navigating the regulatory environment when implementing AI in fraud detection, especially in industries like finance and healthcare, requires meticulous adherence to compliance standards while benefiting from the advantages of these technologies.

Integration complexity:
Harmonizing AI-powered solutions with existing fraud detection infrastructure poses integration challenges. Legacy systems may require substantial updates or replacements to accommodate the new technologies seamlessly.

Cultural shift and change management:
Transitioning from rule-based systems to AI-driven approaches requires a cultural shift within the organization. Resistance to change, fear of job displacement, and concerns about the "black box" nature of AI are obstacles to overcome.

Model robustness and security:
The susceptibility of AI models to adversarial attacks, and the potential for manipulation, pose threats to their reliability. Ensuring model robustness and implementing rigorous security measures are vital to prevent fraudulent exploitation.

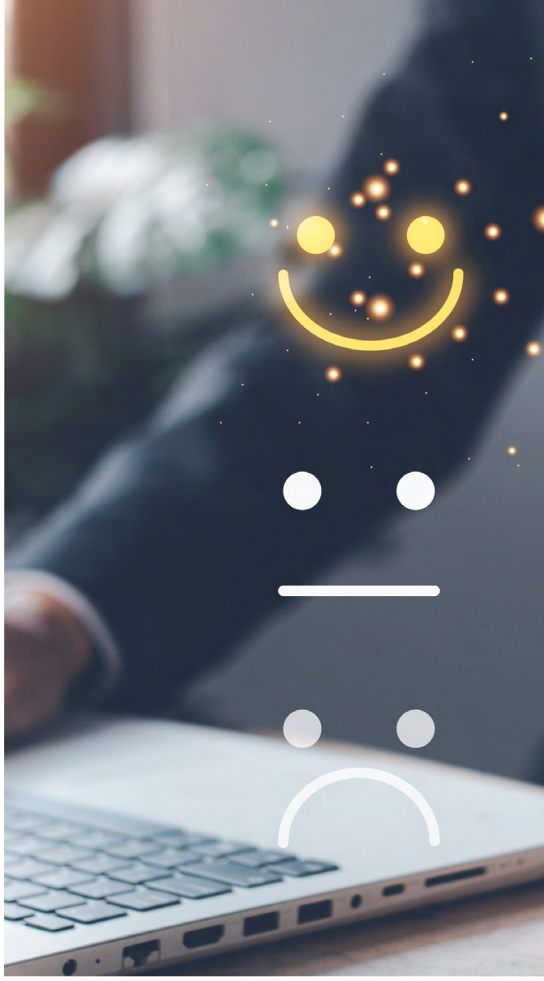
Addressing bias and fairness:
AI models can inherit biases from training data, potentially leading to discriminatory outcomes. Identifying and mitigating these biases to ensure fairness is essential, as biased decisions could lead to reputational damage.

Ongoing maintenance and adaptation:
Continuous monitoring, regular updates, and adaptation to evolving fraud tactics are crucial for sustaining effective performance over time.

Cost-efficiency:
Investing in AI technologies involves costs associated with acquiring tools, hiring skilled personnel, and providing training. Ensuring the investment yields positive returns in terms of fraud prevention is a significant consideration.

Customer experience and digital banking

This year, Cefpro's research team concluded extensive outreach to better understand the key challenges and trends within customer experience and digital banking from a European and US perspective. With such overlap between the two subject matters and geographies, this piece serves as a compare and contrast between challenges and opportunities on the horizon for each discipline.



A key area in each geography was Fintech/startups (Fintech for the purposes of this piece). The nuances observed in each study saw a more collaborative focus from a digital banking and US audience, with the European customer experience (CX) audience focusing more on disruptive capabilities, and staying ahead in such a landscape. The European research highlighted the complexities of fintech/incumbent relationships, identifying more competitive opportunities than collaborative ones. The focus sat within the capabilities of fintech companies to disrupt traditional banking services and offerings.

Customer expectations

As customer expectations continue to evolve - brought on initially by the move of traditional banks to digital-only services during the pandemic – the expectation of even the most traditional consumer evolved almost overnight. With this change came the introduction of large organizations, or "Bigtech" firms launching banking products. Organizations like Amazon have driven demand for instant gratification across a range of services; consumers now expect rapid service and recognize this as synonymous with brands like Amazon and Apple, who continue to enter the market. Fintech, bigtech, and startups are in nature more nimble and agile than traditional banking organizations, allowing them to meet consumer expectations much quicker and adapt. Staying ahead in this market requires significant investment in legacy systems or leveraging a collaborative venture with these nimble firms, as seen in the US research.

Joint offerings

Discussion points in the research for digital banking, which targets a US audience, centered around assessments on how fintechs and incumbents can leverage their joint offerings to maximize customer experience. For example, leveraging the long-standing reputation of a large incumbent bank, which may offer security to a customer, with the agile technology and product offerings of a fintech, diversity in products, and a tailored approach. It was also highlighted in both demographics that the limited compliance experience of fintechs and bigtechs could pose a compliance risk to incumbents, given recent third-party risk regulations stipulating the level of compliance expected.

Personalization opportunities

As consumer demands continue to evolve, organizations are targeting more tailored marketing to broaden their offerings to certain market segments; opportunities exist for mass, group, and individual personalization. Research around personalization brought up a host of opportunities to enhance digital banking and customer experience across both demographics. Both European and US audiences saw opportunities to develop personalized outreach to customers.

AI potential

The potential of AI was an area discussed, and the use of generative AI and broader predictive analytics. More automated technologies allow for a deeper review of customer data to identify trends and customer propensity to leverage certain products. Developing data strategies to source granular data on customers allows for product tailoring based on a range of criteria, including affordability, spending patterns, and more. Developing more tailored and services, could increase customer engagement and build loyalty, a trait not to be underestimated in a digital era where switching providers is increasingly simple.

Generating programs to advance tailoring and personalization is key to staying ahead in a competitive landscape. Leveraging the power of fintechs, as outlined above, could be another opportunity to develop programs and deliver to scale in a much quicker timeframe. Organizations face a balancing

act between advancing digital opportunities while retaining customer relationships and loyalty. Developing digital processes and accessibility is appealing, and even essential, to some demographics, but not all. It is important to stay accessible and retain a "human" element in banking. Customer populations are increasingly complex, with blurred lines between those who expect digital services and those who don't. Traditionally, older people are accustomed to in-person banking. After the pandemic, many people adapted to a digital service, developing a new generation of customers expecting technology to complement the human relationship, not replace it. For a digital experience or journey to be effective, it must be seamless.

Customers are increasingly impatient, expecting instant service and results; loyalty may not hold if their digital journey is interrupted or "glichy". This, again, was an area seen almost equal across geographies, as with personalization, understanding the customer is key. Leveraging the power of AI and other technologies could drive digitalization opportunities. As many larger organizations operate with a high degree of technology debt, implementation of new technologies and integration across systems remains a challenge. More and more, banking organizations are using digitalization as a competitive advantage. Are you keeping up?

As a whole, both demographics were largely aligned. Disparities were evident in the view of fintech, bigtech, and startup organizations, reigniting the competition vs. collaboration debate. The complexity of changes already in place also differs across geographies, with the UK and Europe typically further ahead from a payments perspective due to real-time and instant payment, cross-border, and open banking regulations. The introduction of US payment rails and FedNow may serve to drive the evolution forward in the US and develop more advanced payment practices for customers. Expectations from consumers across both demographics featured a focus on data security, technology capabilities for a seamless digital journey, and personalization of products to open up potential to customers based on their unique factors.

"As consumer demands continue to evolve in the direction outlined above, organizations are targeting more tailored marketing outreach to broaden their offerings to certain market segments; opportunities exist for mass, group, and individual personalization. Research around personalization brought up a host of opportunities to enhance digital banking and customer experience across both demographics".

Customer Experience will take place in London on November 21-22, with Digital Banking in NYC on September 28-29.

Visit www.cefpro.com/forthcoming-events for all information on either event and www.cefpro.com/connect for post-event presentations and video recordings.

Non-financial risk trends in 2023

Incorporating operational and strategic risks to shape the leading risks for the year so far

This year has been tumultuous for operational and non-financial risk teams. After emerging from the pandemic, teams were then gripped by a rise in focus around ESG, global geopolitical uncertainty, and the ripple effects of such volatility. With much of the focus remaining on global economic uncertainty, non-financial risks must remain top of mind to ensure the security of global organizations.

TOP NON-FINANCIAL RISKS FOR AS OUTLINED IN CEFPRO'S NON-FINANCIAL RISK LEADERS REPORT

Source: CeFPro's NFR Leaders

1. Cyber risk

2. ESG (inclusive of climate risk)

3. Geopolitical risk

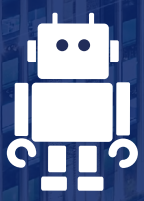
4. Third-party risk

5. Resilience and business continuity

6. Compliance and regulation

7. People risk

8. Fraud



9. Technology risk

10. AML and financial crime

MOST IMPORTANT EMERGING RISKS OVER THE NEXT 5 YEARS

Source: EY/IIF global bank risk management survey

Concern to CRO

- **91%** Climate risk
- **83%** Length and depth of global economic recovery
- **68%** Pace and breadth of change from digitization
- **62%** Industry disruption due to new technologies
- **60%** IT obsolescence/legal systems
- **55%** Integrity of data/data destruction
- **53%** Use of ML/AI
- **53%** Industry disruption due to new entrants
- **53%** Data privacy
- **51%** Model risk related to ML/AI

74%

The number of respondents to a Bank of England survey deemed cyber-attacks to be the highest risk to the financial sector in the short and long term

Source: Bank of England

44%

The number of banking customers who rate environmental and social issues as very important

Source: RBR Social responsibility: The future of mainstream banking

49%

Geopolitical risk is seen as a major emerging risk for CROs - down from 60% in 2019

Source: EY

82%

When prioritizing third-party ESG risks, 82% report moderate to very high levels of awareness/focus on ESG issues

Source: Deloitte

£1.2 b

Over £1.2 billion was stolen through fraudulent activity in 2022, down 8% from 2021. The number of UK fraud cases was also down 4% to almost 3 million cases.

Source: UK Finance

LOOKING AHEAD TO 2023, WHAT TYPES OF FRAUD IS YOUR ORGANIZATION MOST CONCERNED ABOUT?

Source: Comply Advantage

41%	Investment scam
41%	Tax fraud
39%	Credit/debit card fraud
36%	Identity theft
31%	Synthetic identity fraud
31%	Phishing
25%	Elder fraud
22%	Romance fraud

The growth of social media and its impact on fraud

Ionela Emmett
Senior Manager, Financial Crime Controls, Risks & Policy
ICBC Standard Bank Plc

During the pandemic and subsequent lockdowns, the number of users on social media soared, and they continue to be high as more people become dependent on online services. Whether for business or personal use, there is a social media app to cater to all requirements, requiring users to create an online profile. It has become more commonplace for people to be scammed out of money online as fraudsters can impersonate a victim's bank, employer, or even law enforcement. As techniques and tactics continue to evolve, victims aren't being naïve but are being taken advantage of. Therefore, how do they remain protected while online?

How are people affected by the relationship between social media and fraud?

In recent years, social media platforms have grown exponentially, with some new and others making interface changes; for example, Twitter rebranding to X. Developers see more people engaging with social media, so they continue to design new platforms to diversify audiences in a crowded space. As this growth continues, marketing companies and businesses are joining social media platforms to boost engagement and business revenues; this can be seen with the volume of adverts consumers are exposed to on social media platforms. Recently, social media giant Meta introduced Threads to compete against X, attracting 5 billion users in its first week, overtaking the sign-up to ChatGPT for the same period.
Results from a 2023 study by Meltwater show that 64.6% of the world's population are using the internet, with 59.9% on social media. These figures are not only up from previous years but show that more than a third of the population has an identity online where they could be at risk of harm. Often, people share their personal information without a second thought, including home address, place of work, family members' names, birthdays, and other personal details. People forget this information isn't just shared with friends and family but with strangers too. Despite privacy settings attempting to protect a user's data, strangers can still see their information.

Data security

Additionally, social media app updates can change privacy settings, and users may not realize their information's now visible. Without a doubt, a pool of fraudsters are continuously looking to harvest personal information to use for illegal activity. The internet and social media allow criminals to hide behind anonymity, creating fake personas to enact the fastest response from victims to perpetrate the crime even quicker, making it difficult for law enforcement to identify and trace fraudsters; this could be considered a cybercrime. Financial institutions are seeing a vast amount of people being contacted directly through social media. Platforms like WhatsApp and Messenger are seeing users receive direct messages attempting to scam them by selling products and opportunities to make investments and buy shares and cryptocurrencies. Romance scams are also a huge problem, befriending someone and then introducing a more personal relationship lures victims into a false sense of security, enabling fraudsters to exploit them.

GDPR legislation has been at the forefront of aiming to protect how personal data is stored by companies online, with many people familiar with the term but not their consumer rights. This right is typically waived on social media despite being told personal data is not sold or shared; website cookies allow tracking personal information to create targeted ads and then sold to third parties for a price. The fraud factor can become an even higher threat as fraudsters and social media companies harvest and share personal information.

Who is responsible when a victim is scammed via social media?

Arguably, social media platforms are enabling access for fraudsters to contact victims, engage with them, and harvest their information. On platforms like Facebook and Instagram, marketing adverts are shown to users, yet the vetting process is unclear and leaves some room for interpretation. Advertisers sell high-end products at significantly reduced prices or investments in specific companies, and as they are on what appears to be a safe social media site, victims see them as genuine businesses. The responsibility should lie with the social media companies as their due diligence processes do not

capture the fake businesses, therefore allowing them on the platform. There is also an argument that social media companies should be held at least partly responsible for the marketing information shared on their platform and the access they provide allowing people to be contacted directly.
This can make social media a scary place for the average user, as the line between legitimacy and criminality has become blurred and uncertain.
Under the new release of the Payment System Regulator requirements, banks are expected to support victims and reimburse them in genuine situations of online scamming. If customers are warned about a detected scam or fraudulent activity but wish to continue, a bank has few powers to decline the request after warnings.
But who is to really blame once a transaction is processed? The victim who was trying to buy something they thought was legitimate, the bank for helping process the transaction or the platform that advertised the scam in the first place?

How do you see this situation being mitigated?

The long-term solution is to reduce the number of fraud cases overall, not just to encourage victims to claim the money, as this makes online fraud persist and grow. Despite education and awareness campaigns online and on TV, it doesn't appear to be lowering the level of cybercrime.

To do this, social media platforms must explore some level of KYC and data-acquiring processes. Hence, fraud could be tackled in the early stages of fraud. A proactive approach from social media platforms will be prevention, encouraging users to be aware of red flags.

It will be tough for social media companies to put controls in place where they must vet the marketing companies posting ads on their platform. The costs and workforce associated with this would be unattainable, but a minimum level of vetting enforced could make a gradual shift. This could change the mentality of fraudsters as they would know they have a high risk of being detected. Arguably, the governments needs to step in to enforce changes.
The Online Safety Bill was initially drawn up to tackle cybercrime, with investment fraud recognized as one of the highest threats in the UK. However, when it came to the consultation of the Online Safety Bill, it became focused on the abuse and exploitation of young people. Although this was needed, other vital risks to online safety should be addressed.

All people are at risk of online fraud: fraudsters don't discriminate; as long as someone has internet and social media access, they are a potential victim.

Fraud and Financial Crime USA will be held in New York City in March 2024. Hear from industry experts on a range of financial crime challenges and opportunities. www.cefpro.com/fraud-usa

Keith Davies
Group Chief Risk & Compliance Officer
Admiral PLC

ESG: Mitigating reputational risk of "greenwashing"

During CeFPro's Risk EMEA 2023 Convention, Keith Davies, Group Chief Risk and Compliance Officer at Admiral PLC, took part in a fireside chat on enhancing the oversight of social programs and mitigating reputation risks with potential greenwashing. These are some of the key points'.

How are firms currently dealing with incorporating environmental, social, and governance (ESG) into a sustainability strategy?

Firms initially focused their sustainability initiatives on managing the "outside-in" risks to which they are exposed – most notably meeting regulatory requirements and mitigating the risks that climate change could present to operations, financial investments, and retrospective litigation. However, businesses are increasingly seeing that their own "inside-out" sustainability stance – its own impact on society and the environment – is key to an organization's long-term performance – with a positive sustainability stance representing opportunity by:

- Increasing demand by aligning products and services with customers' evolving expectations, and by improving brand positioning.
- Reducing costs by lowering energy consumption and associated costs, and reducing borrowing costs (for example, better ratings or access to alternative financing sources such as green loans), insurance costs, and costs of third-party providers.
- Improving the employee proposition and productivity by attracting, motivating, and retaining employees by focusing on how well a company looks after its staff and/or addresses key social and environmental issues.
- Enhancing a firm's brand, reputation, trust, and social license to operation – with authentic delivery and communication on sustainability issues positively impacting all stakeholders' perceptions.

However, in order to fully capture the opportunities sustainability can present – the approach has to be strategic, holistic, authentic, and match the purpose and beliefs of the company to increase long-term value. It can no longer be a one-off or "on-the-side" project but needs to be fully aligned with the firm's values and strategy to prevent the reputational risk of "greenwashing" and not "walking the talk". It also needs to be holistic across all the areas of ESG in order to manage the conflicts that can arise, for example, the "just transition" risk that adopting climate mitigation measures could result in economic harm and social issues, such as unaffordability or exiting certain suppliers.

Should third parties be held to the same standards as your organization?

A holistic approach to sustainability means firms cannot just think about their own sustainability position but also that of their supply chain and partners; there are two main reasons for this. The first is that suppliers who adopt a robust sustainability approach are more likely to prosper (and best support their clients) in the long term – both because they have taken account of "outside-in" risks to their business (for example, created arrangements in case of

climate events), and because they themselves will benefit from the advantages listed before. The second is stakeholders typically view the different components of a firm's value chain as an extension of the firm, both in terms of service delivery and behavioral standards. This means businesses increasingly need to work with third parties who align and support the delivery of their own ESG objectives. The long-known view that firms can outsource activities but not responsibility has become that firms can outsource activities but not responsibility or reputation. This trend will continue as companies increasingly need to report not just on their own internal impact on society and the environment but the consolidated impact of the whole value chain.

This creates the practical issue of companies assessing the sustainability credentials of the value chain, which can raise a number of issues. Firstly, while firms can readily incorporate sustainability criteria when selecting new partners, making such factors part of the selection process and contractual obligations, it is harder to impose required standards into existing contracts, both from a legal perspective and because suppliers will need both time and investment to transition to the new standards. Secondly, the reality is that larger suppliers will not vary their arrangements for individual firms – although, in most cases, the requirements of their main clients will mean they will have a sufficiently acceptable sustainability approach. Thirdly, firms can have hundreds of suppliers and partners and do not have the time and resources needed to assess whether all existing suppliers meet the required standards. Firms will need to adopt a risk-based approach potentially along the following lines:

- For lower-risk providers, firms can potentially look to leverage ESG ratings and controversy scores to give a simple indicator of the sustainability risk that suppliers may pose the purchasing company's sustainability and reputational status.
- For medium-risk suppliers, this process could be enhanced to include additional due diligence questionnaires and reports on key sustainability metrics.
- For the highest-risk big providers, firms should undertake detailed reviews of key metrics, onsite audits, and management meetings with their largest providers.

However, this approach also requires companies to assess the risk that suppliers pose to their own sustainability credentials. This depends on the importance of the arrangements to the purchaser in terms of financial cost and impact on sustainability targets but also on the extent to which an incident at the supplier would reflect on the purchaser's brand and reputation as reputationally "you're only as strong as the weakest link in your chain".

Can holistic scores really be given for ESG to third parties?

This raises the question of whether, and how well, ESG ratings can capture the overall sustainability of a supplier?. It is true scores vary considerably across rating agencies – both in terms of the weighting they place on different factors (which may mean they differ from a user's own value) and, in some cases, measure the outside in risk that ESG factors can have, rather than the actual nature of a firm's own sustainability stance. However, they are the only realistic option to assess a wide range of companies in a simple and standardized way and can be a good starting point. For example, the chance of lower-risk suppliers, with a relatively good ESG rating, negatively impacting the sustainability standing of a purchaser is low – meaning that firms can target their assessment on more material and/or higher risk suppliers. Moreover, the quality of ratings should improve as the quantity of firms' data and rating approaches improve, and as more granular approaches allow firms to better assess how third parties align with their values in specific areas.

What are the best ways of managing risks and regulatory requirements regarding reputational damage due to "greenwashing" allegations?

Greenwashing is the term used when companies promote environmental and sustainability stances that they either don't do, never intend to do, or can't prove they've done. It creates a significant reputational risk when firms are shown to not meet stakeholder perceptions and indeed can lead to regulatory sanction if found to be deliberately misleading. In order to avoid greenwashing, companies must be authentic in designing their sustainability strategy and making sure it aligns with their purpose, values, and strategy so that sustainability is part of the DNA, heartbeat, and day-to-day activities of the organization. They must also implement a series of governance and culture measures to roll out and support delivery of their sustainability approach, including:

- Board accountability and oversight of sustainability.
- Sustainability considerations being embedded into strategy and key decision making.
- Education on sustainability approach.
- Sustainability policies, procedures and codes of conduct, objectives, appraisals, and remuneration being linked to sustainability targets.
- Management and contingency for sustainability risks.

How should businesses evolve their approach to sustainability?

The overall shape of a firm's sustainability strategy should not change significantly from year to year. However, as markets, stakeholder expectations, and societal preferences continually evolve, companies should review all components of the strategy on a regular basis. A firm's sustainability approach should flex as societal expectations change – recent examples include how attempts to reduce motor emissions (For example, the London ULEZ zone) may need to be tempered in the current cost of living crisis, and how munitions have moved from being a SIN-stock before the Ukraine war to now being seen as supporting democracy. As a result, while continuing to be guided by a firm's values and purpose, Boards do need to be mindful of changing expectations of stakeholders and potentially alter their sustainability stance.

ADVERTORIAL

Transforming third party risk management

Panorays

Dov Goldman
VP, Risk Strategy
Panorays

How can an organization improve resilience while developing infrastructures to manage third-party risk?

An effective third-party risk program begins with support from the business and becomes integral to the organization's decision-support process for choosing, managing, and (when needed) ending supplier and partner relationships.

What, for you, are some key principles of a third party or digital supply chain risk program?

It all begins with truly understanding the inherent or business risks of each third party relationship. The third party risk team must collaborate with the business to profile each relationship, then identify the areas of "material risk", which are the specific potential problem areas and, therefore, the controls that must be tested.

The inherent risk rating helps the team to prioritize each relationship and decide what level of assessment to perform, while the more detailed material risk information will guide exactly what to assess.

How are you seeing technology advancing third-party risk and supply chain challenges?

The challenge for many years was to model third party risk assessment and management processes in great detail and use technology to accelerate them. Today, there are platforms that successfully respond to these needs. Many companies share data with and rely critically on more third parties than ever before. A multitude of SaaS vendors has replaced so many traditional on-premises systems, creating a much bigger "attack surface" and a huge resource challenge. Accelerating manual processes is no longer enough.

Artificial intelligence (AI) tools will soon fill this gaping hole by automating many aspects of third party risk assessment. Risk evaluators will be aided by smart platforms that will act as true decision-support tools.

Risk evaluators will be supported by well-tuned AI systems to manage large numbers of assessments, thereby supporting business and their appetite for SaaS-driven tools while continuing to protect data security privacy.

For more information, click here

Hear from Dov and the Panorays team at Third Party & Supply Chain Risk: Cross Sector. Dov is charing Day One of the event!

ADVERTORIAL

The strategic imperative of resilience in the financial services industry

The financial services industry faces unique challenges that stem from its role as both a custodian of assets and capital but also massive amounts of user data. Navigating and thriving in today's fast-evolving landscape requires an unwavering commitment to building strong digital defenses in order to maintain resilience. In an era dominated by digital transformation, companies in this industry find themselves as drivers of this transformation, adopting digital applications to improve the customer experience on the front end while bolstering defenses to mitigate cyber risk on the back end. Concurrently, they are building enterprise resilience and strengthening organizational culture to allow for business growth and a competitive future.

As we assess the future of the financial services industry, which is the cornerstone of the global economy, it is important to understand how next generation technology will be leveraged to maintain holistic business resilience.

Organizational resilience

To thrive in unprecedented circumstances is to have organizational resilience—a key pillar that is highly prioritized in the financial services industry. The global pandemic taught us that, even when crises or major disruptions arise, keeping employees as informed and focused as possible results in resilient dynamics within the organization.

Clear and consistent employee communications and maintaining a positive company culture contribute to a more engaged and productive workforce that is invested in the values and policies of the company. Organizational resilience is also a key factor in determining whether employees at all levels can help their organization successfully navigate a crisis or disruption.

The value of technology in building resilience

A survey commissioned by Dataminr and conducted by Economist Impact found that the financial services industry overwhelmingly ranked digital assets—such as data, websites and IT platforms—as number one when asked about priorities for advancing their organization's business strategy. Sixty-one percent said they feel "very prepared" to respond to cyber risk. This can be attributed to recent high-profile breaches, which affected consumers and institutions and led to heavy investments in securing digital networks and staff training on how to protect data better and identify and counter hacking and fraud.

Protecting digital assets is not just about bolstering the security of an institution's digital infrastructure. Forty-two percent of financial services respondents said managing physical security risks is one of the top three strategies for protecting digital assets—a greater proportion than their peers in the energy, manufacturing, tech, and retail industries.

Harnessing artificial intelligence

Eighty-five percent of respondents believe that AI will positively impact their organization's ability to thrive and create value in the next three years. Leveraging AI to better protect financial services companies' physical and digital assets and its user data is a big driver of that value. AI is generating business value in other areas as well. For example, it can enhance a firm's customer experience. Machine learning and new advanced AI techniques have been used to conduct real-time analysis of customer transactions with remarkable precision and speed. Firms can then accurately calculate default risks, resulting in reduced credit risk, allowing them to extend cheaper loans to customers more quickly.

To thrive, regardless of circumstances, is to be resilient. In a dynamic and unpredictable business environment, operational, organizational, and technological resilience are essential for ensuring sustainable growth and success for financial services companies. Whether facing internal crises or disruptive external forces, resilient leaders and organizations understand that real-time information yields critical lead times and insight and informs decisions. This, paired with the adoption of next-generation technology, gives organizations the best opportunity to remain competitive, trusted, successful, and resilient.

A new regulatory focus in compliance: Off-channel communications

Sabeena Liconte
Chief Compliance Officer
ICBC Standard Bank

Late 2021 marked the emergence of a new regulatory focus in US financial services, signaling new enforcement priorities and important lessons for compliance risk professionals operating in the US capital markets. The Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) entered into a settlement totaling $200 million against JPMorgan Chase for widespread recordkeeping violations due to business-related messages sent using apps on employees' personal devices. The SEC and CFTC coined these messages "off-channel communications" to refer to the use of unapproved communication channels by a financial institution's employees to discuss business outside of traditional recordkeeping processes. Examples include text messages, social media, or other online messaging services (such as WhatsApp, WeChat, or Signal).

Enforcement and settlements

Federal regulators in the US have been steadily turning their focus to the use of off-channel communications, and a flurry of enforcement activity, public pronouncements, and other related activity has ensued as a result of this new enforcement focus.

- On September 27, 2022, the SEC settled charges totaling $1.1 billion against 15 broker-dealers and one affiliated investment adviser for widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications. A whole host of firms were sanctioned and received penalties ranging from $10 million to $125 million.
- On September 27, 2022, the CFTC settled charges totaling $260 million against swap dealer and futures commission merchant ("FCM") affiliates of 11 financial institutions for failing to maintain, preserve, or produce records that were required to be kept under CFTC recordkeeping requirements, and failing to supervise matters related to their businesses as CFTC registrants diligently. The impacted firms were sanctioned and received penalties ranging from $6 million to $100 million.
- In a memorandum issued on September 15, 2022, by the U.S. Department of Justice ("DOJ"), Deputy Attorney General Lisa Monaco noted that the increased use of messaging platforms on personal devices, including those that offer ephemeral and encrypted messaging, pose "significant corporate compliance risks, particularly as to the ability of companies to monitor the use of such devices for misconduct and to recover relevant data from them during a subsequent investigation". As such, when evaluating a corporation's compliance program for purposes of a potential resolution with the DOJ, prosecutors should consider whether there are effective policies and procedures in place to ensure that business-related communications are preserved.
- Recent revisions to the DOJ's Evaluation of Corporate Compliance Program guidelines in March 2023 advises prosecutors to assess corporate governance approaches concerning personal devices, communications platforms, and messaging applications in evaluating corporate compliance programs and making charging decisions. An assessment should be performed to ascertain whether the use of such modes of communication are tailored to the corporation's risk profile

and specific "business needs" and whether "business-related electronic data and communications are accessible and amenable to preservation by the company." Prosecutors should evaluate:
    - What channels of communication are used, or are authorized to be used, to conduct business as well as the mechanisms the company uses to manage and preserve data within each of the channels.
    - The policies and procedures that allow companies to monitor, preserve and review business-related communications on personal devices.
    - The risk management policies in place, including consequences for employees who refuse the company access to their business communications.
- On March 23, 2023, Assistant Attorney General Kenneth Polite Jr. stated in a keynote address for the DOJ that "prosecutors will not simply accept a company's inability to produce messages from third-party applications without adequate explanation.".
- The SEC launched in early 2023 a targeted sweep focused on private equity and hedge fund firms' use of personal devices and the extent to which those communications were being maintained under the recordkeeping obligations of the Investment Advisors Act of 1940.
- On May 11, 2023, HSBC Securities (USA) Inc. ("HSBC") and Scotia Capital (USA) Inc. ("Scotia Capital") paid a combined $37.5 million in fines to settle actions with the SEC for violations arising from their failure to maintain and preserve employees' business-related communications on personal devices. HSBC agreed to settle with the SEC and pay a $15 million fine, and Scotia Capital agreed to settle with the SEC and pay a $7.5 million fine. The press release regarding the settlements stated that there were "widespread and longstanding failures by both firms and their employees to maintain and preserve electronic communications," but it noted that the penalties were reduced in consideration of the voluntary self-disclosure and remediation efforts undertaken by both firms.
- The CFTC separately settled with Scotia Capital USA Inc., an FCM, and the Bank of Nova Scotia, a provisionally registered swap dealer, and Scotia Capital USA Inc., an FCM, for $15 million, for recordkeeping and supervision failures due to the widespread use of unapproved communication methods.
- On August 8, 2023, the SEC settled charges totaling $289 million against 10 firms operating as broker-dealers and one dually registered broker-dealer and investment adviser for widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications. Firms were sanctioned and received penalties ranging from $9 million to $125 million.
- On August 8, 2023, the CFTC settled charges totaling $260 million against swap dealer and futures commission merchant affiliates of 4 financial institutions for failing to maintain, preserve, or produce records that were required to be kept under CFTC recordkeeping requirements, and failing to supervise matters related to their businesses as CFTC registrants diligently.

Each of the settlements targeting off-channel communications involve long-standing books and records requirements of the SEC and the CFTC regulating the maintenance and preservation of documents. Specifically, Section 17(a)(1) of the Securities Exchange Act of 1934 authorizes the SEC to issue rules requiring broker-dealers to maintain and preserve records as necessary or appropriate in the public interest. The SEC adopted Rule 17a-4 to mandate that broker-dealers preserve all communications received and all communications sent relating to the firm's business. The Commodity Exchange Act and CFTC rules, like CFTC Rule 1.31, impose similar requirements on CFTC registrants.

Lessons Learned

There are valuable lessons that can be learned by compliance risk professionals from the above enforcement activity and guidance issued by the DOJ. Financial services firms can:

- Adopt a policy identifying approved methods and non-approved methods of communication, including on personal devices.
- Ensure any permitted mode of communication is monitored and subject to review and archival.
- If an employee receives a business-related communication on a personal device, have a protocol in which they are required to move that correspondence to a company-monitored system. Where it is impracticable or impossible for the employee to do so, (a) mandate that the employee notify and document for your compliance division why compliance with the procedure is not possible and (b) have the employee promptly record the details of what was discussed in a company monitored system.
- Train staff on applicable policies and procedures.
- Require employees to attest that they are in compliance with firm policy periodically.
- To the extent that an employee is provided with a company phone, either block texts and third-party messaging systems or archive and maintain records of communications sent via text or a third-party messaging system.
- Document incidents of non-compliance and implement effective systems of escalation and remediation.

The onslaught of recent enforcement activity in the off-channel communication space empowers compliance risk professionals with valuable insight into how the regulators are thinking about such modes of communication and underscores the targeting of such communications as a new regulatory priority. As such, financial service firms should regard the current environment as imposing on them an affirmative duty to proactively implement controls to effectively "police" for such activities; adopting a policy of inaction is simply inconsistent with regulatory expectations today and is simply far too costly of a strategy to employ.

1. https://www.justice.gov/opa/speech/file/1535301/download.
2. https://www.justice.gov/criminal-fraud/page/file/937501/download.
3. https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-address-global.
4. Advisers Act Rule 204-2(a)(7) and 206(4)-7, 17 CFR §275.204-2 and 17 CFR §275.206(4)-7.
5. https://www.sec.gov/news/press-release/2023-91.
6. https://www.cftc.gov/PressRoom/PressReleases/8699-23.

ADVERTORIAL

The most significant step you can take to transform your CX

Andrew Stevens
Principal, Banking and Financial Services

quadient

How would you describe the current state of customer experience in digital banking?

It's not great, to put it politely, but it isn't the fault of the digital teams. Banking has never really been about CX before now. Banking leaders have always seen the digital revolution as a way of driving transformational change for revenue-related purposes. Digital and mobile banking really started to mature shortly before the global financial crisis, when cutting costs was the top priority, so major investments were made in areas that reduced the need for high-cost customer interactions, such as in-person customer care at local branches. The digital strategy hasn't really altered since, and it now needs a revolution rather than evolution to fix it.

What are some of the risks associated with current CX processes?

The obsession with empowering customer self-reliance in managing their money is the riskiest CX approach right now. There's certainly value in enabling the customer to perform basic tasks without help but pushing the customer too far in assuming they always want this approach can have unintended consequences. Every bank wants to form positive, long-term relationships with their customers – it's what keeps customers happy owning products that aren't at market-leading rates. But forming that relationship with someone you've never met is difficult, and the ease at which we can all move our money today (thanks to the same amazing digital technology) means that it's far easier to lose a self-service customer without any warning.

What are your 3 key tips to enhance CX?

- **Your customers don't want what you wish they'd want.** You want them to love you while they handle all of their affairs alone because that's a low-cost way of running a business. Customers want to feel loved and appreciated and, most importantly, advised. Improving your CX means considering the revenue as the reward, not the aim.
- **Be brutal with your technology.** It's easy to explain poor experiences by pointing out how expensive the "right" approach would be or how many IT platforms are involved. Customers don't care about the excuses, so banks need the same approach. That means being willing to rip out IT solutions that don't serve the customer properly and having the nerve to admit that recent purchases (perhaps made in desperation during the COVID-19 pandemic) aren't going to deliver for the customer in the long term.
- **Communication is key.** If you can't interact with your customers in an engaging, personalized, and deeply meaningful way that supports and educates them at the right time and on the channel they prefer, then you're ruining all of your CX efforts in that all-important final mile.

Without giving too much away, have you seen any areas where organizations excel in this, in which case, what are some of the key features that drive that success?

Digital proactivity is an emerging trend in banking right now. The organizations really making waves in CX are those that are always monitoring their customers' financial affairs and immediately communicating with them with actionable intelligence.

For example, many of us are accustomed to receiving a smartphone push notification when we spend money on a card. The best banks are making this interaction valuable to us, explaining what that transaction means for our projected spending and alerting us if the analysis suggests we need to change our spending patterns.

To do this properly, banks need to be able to understand the customer and act in a highly personalized way to interact with them in real time. That usually requires complex data being pulled from multiple sources and advanced communications being composed and delivered at scale, always on the customers' preferred digital channel.

www.quadient.com/cxm

Global CeFPro® Research Report

FINTECH LEADERS

January 2024

We want to hear from you, Fintech Leaders 2024 voting now open!

Submit your votes today

www.fintech-leaders.com

****All responses are anonymous***

Participate in our short online survey and provide critical insights into the key opportunities, investment priorities, and benefits and challenges that financial technology has brought to your institution, plus the opportunity to nominate your top solution provider as a Fintech Leader in our ecosystem ranking.

"Our firm uses {Fintech Leaders} to inform our enterprise risk and control strategy and broaden our near-term and long-term management and investment views."
Head of Operational Risk, *Cross River Bank*

All respondents will receive a 15% discount off their next CeFPro Events registration, and receive a free copy of the report upon release in 2024.

Fintech Leaders is endorsed by Senior Risk Professionals around the world representing established financial institutions:

BNY MELLON · ING · CRÉDIT AGRICOLE · cross river · COASTAL FINANCIAL CORPORATION · SoFi · BAILLIE GIFFORD · NatWest Group

www.fintech-leaders.com

Identifying concentration risk: Resilience, efficiency, and scalability

Richard Brown
Director Compliance Risk Management
USAA Federal Savings Bank

On June 6, 2023, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency (OCC), and the Department of the Treasury recently issued a final guidance memo on the management of third-party risk (TPRM). In addition, on April 25, 2023, Canadian regulators from the Office of the Superintendent of Financial Institutions (OSFI) released a revised version of its B-10 guidelines for TPRM. Both mention that financial institutions, including banks, credit unions, and other lenders, should be cognizant of the risks posed to the financial organization (institution-specific concentration risk) and the financial system (systemic concentration risk) of overreliance on a single third party.

For this discussion, we will use the term "concentration risk" to refer to the risk of loss or harm to a financial institution from overreliance on a single third party, subcontractor, or geography for multiple activities. While reliance on third parties is ubiquitous in the current environment, it is sometimes more difficult to clearly delineate when a relationship has strayed into overreliance. Some key factors to consider are when the third-party relationship poses risks to the resilience of the financial institution, risks to the efficiency of the financial institution's operations, or risks to the scalability of the financial institution's performance against the institution's strategic plan. But first, an organization must set a firm foundation for evaluating its vendors, considering the relative risk posed by outsourcing each process the third party provides.

Know Thyself

The Greek philosopher Socrates is credited with saying, "to know thyself is the beginning of wisdom". In evaluating the risk posed by third parties, it is also wise to know the internal processes that may be outsourced to third parties before any meaningful analysis can take place.

First, a financial institution must have a comprehensive inventory of the processes that exist within the financial institution's operations to evaluate the "critical" processes that must be completed to achieve product and service delivery. These processes should be mapped out thoroughly so that each process can be appropriately evaluated for inherent risks, tied to a framework of controls, and then assessed for residual risks.

Not all financial institutions operate similarly, but there will be similarities in many critical functions. For example, for highly regulated banks in the US, the delivery of regulatory-required disclosures to consumers will be a critical process across most, if not all, institutions. The assessment should also result in a residual risk rating of the process for operational risk. In areas where this residual risk rating is high for critical functions, outsourcing these processes to third parties may improve a financial institution's ability to meet its customers' needs if the third party adequately mitigates certain risks. However, outsourcing processes also carry the risk that reliance on the third party can increase risk in core areas. These risks are aggregated into resilience, efficiency, and scalability threats in the sections below.

Resilience concentration risk

The chief regulatory concern for concentration risk in a single third party or similar arrangement is that the arrangement jeopardizes the resilience of the financial institution should a disruption or incident occur, whether internal or external. To assess whether concentration risk to resilience is unacceptable for your institution, determine whether there are scenarios where a loss event could impact the delivery of the core service provided by the third party on behalf of the institution. Then, review the mitigating controls to decrease the probability of the loss event (or that may reduce the impact of the loss event). If the result of this assessment is that the use of a particular third party or parties located in one geographic area results in risks to service delivery outside of your organization's appetite, then further diversification of third-party relationships should be considered.

For example, if a financial institution were to house all its data at a data center in an area prone to hurricanes, would it be lost if that one area was devastated by a catastrophic storm? Similarly, if the data was housed with the same data storage vendor, and that vendor were to be compromised by ransomware deployed at all sites maintained by that vendor, would there be backups available for the financial institution to recover? In both scenarios, strong regulatory frameworks protecting this information require

the financial institution to ensure that it has safeguards in place to recover from these events. Controls to mitigate this risk would be backup data centers in areas where natural disasters were not prevalent or the presence of cybersecurity backup protocols to protect against malicious encryption.

Scenarios that threaten resilience can quickly point out relationships with unacceptable concentration risk. Additional resilience threats may include:

- Noncompliance with legal and regulatory requirements.
- Weak financial condition or management that may threaten the viability of the third-party.
- Inadequate staffing or operational management of the third-party resulting in service failure or delay.
- Weak information security/management information systems at the third-party.
- Inadequate business continuity and disaster recovery plans at the third-party.
- Heavy reliance on subcontractors or inadequate oversight of subcontractors in the third-party.
- Potential conflicts of interest or contractual arrangements with other parties.

Efficiency concentration risk

Concentration risks that threaten efficiency include scenarios where using one third-party supplier may result in a less effective spend ratio relative to performance expectations. Efficiency risks may emerge from budget constraints, net revenue goals or targets, or productivity goals the financial institution has set. To assess whether concentration risk to efficiency is unacceptable for your institution, determine whether there are scenarios where the impact of using a different supplier could provide delivery of the core service provided by the third party with a smaller impact to the budget, or with greater operational productivity.

For example, suppose a particular third-party vendor involved with providing legal services initially offered services at a discount to establish a relationship. In that case, those discounts may be gradually rolled back over the course of several contract negotiations as market share or the caseload increases. Perhaps the vendor performed well under a lower volume of cases but struggled to maintain similar performance standards under higher volumes. Controls for this risk include a vigilant review of spending benchmarked over time, strong oversight of service level agreements and objective performance, and frequent market analysis to find other competitive third parties. Resulting mitigation may result in rebalancing the use of the third party with internal resources or competitor third parties. Common efficiency concentration risks include:

- Third-party cost exceeds employee cost.
- Third-party cost exceeds competitor third-parties.
- Third-party performance fails to meet service-level objectives.
- Competitor third parties exceed third-party performance.
- Competitor third parties or internal resources provide economies of scale.

Scalability concentration risk

Concentration risks to scalability describe scenarios where using one third party may result in outcomes that are satisfactory for current needs but fail to meet future strategic objectives or metrics. For one example, the potential growth presented by generative AI and machine learning technologies represents strategic opportunities for financial institutions. Live contact center interactions can be increasingly handled by sophisticated chatbots capable of processing multiple languages at high accuracy rates 24-hours a day. Continuing to use live agents may present inefficiencies in terms of spend in a changed technological environment (efficiency risk). It may decrease customer satisfaction in the long run if response rates and quality of interaction can be matched or exceeded by AI (scalability risk). Controls to mitigate scalability concentration risk include developing strong modeling programs to project market conditions that may change third-party risk management decisions and ensuring that the financial institution's board of directors has insight into third-party processes that may affect strategic goals. Common scalability concentration risks include:

- Technological change requires business adaptation.
- Business growth strategy requires changes in output.
- Geopolitical risks change risk calculation.
- Proprietary systems or skillsets (intellectual property) require protection.

Concentration risk assessment

With some common risks in mind that factor into TPRM, the calculations to determine if the risks are within risk appetite become possible. After aligning the outsourced services with internal needs and resources, concentration risk is easier to identify when risks are aggregated into resilience, efficiency, or scalability risks. These categories allow financial institutions to compare third parties along similar metrics and performance indicators and identify alternatives that serve the institution.

Visit www.cefpro.com/forthcoming-events for a full break down of our global events, including Vendor & Third Party Risk USA and Europe, taking place June 2024 in NYC and London.

ADVERTORIAL

Three challenges and two answers for third-party and supply chain risk

Jeffrey Wheatman
Cyber Risk Evangelist

BLACK KITE

It may well be the case that third-party/supply chain risks are the biggest risks that most organizations aren't adequately managing. As long as I've been in cybersecurity, CISOs, and their teams have focused internally on securing their own environments. And they have, by and large, made a lot of progress. Now, when they think they can sit back and take a breath, they are confronted with new problems, most of which they have little authority or ability to control – risks that accrue from business partners. CISOs can be perfect and yet still be exposed due to the risks inherent in business relationships via third-party and supply chain partners. Their risks have now become your risks.

Three challenges:

- **Your partner risk is now your risk:** Most organizations don't really understand the risk of their extended ecosystems. Partnerships, both digital and physical, grow ever more complex. Understanding points of failure, critical choke points, and significant risk exposure keep getting harder, with cascading and concentration risks making the risk all the greater and harder to understand; you can't manage what you don't understand.

- **Many more inputs are now deemed material:** Third-party and supply chain risk used to be simple. It usually went through if legal and finance were OK with the deal. Now, cybersecurity, audit, compliance, IT, and supply chain teams (among others) are getting involved, and as we know, the more variables, the harder it is to make defensible decisions. ESG, contractual requirements, and cyber insurance are part of the decisions about managing third party risk. And the reality is much of the data is incomplete and low fidelity.

- **Point-in-time snapshots are NOT enough:** Up until recently, the lion's share of assessing risk in the extended ecosystem was based on questionnaires. In other words, you asked partners what they were doing to ensure their cybersecurity and risk resilience, and we basically took them at their word. Assuming the questionnaires were accurate in the first place (which is a dubious assumption at best), every day that passes makes them less accurate and less useful for making decisions.

Two solutions

- **Require more visibility into your ecosystem:** You need to work more closely with business stakeholders. You need to understand where the data is, where it's being used, shared, stored, and processed. Which partners would have the greatest impact on your business if they were hit with a DOS, ransomware, or data theft? In other words, where in the ecosystem are you most exposed? You can answer this question by working side-by-side with your business stakeholders.

- **Implement high fidelity, standards-based, business-driven, real-time monitoring:** Point-in-time snapshots are useless and always have been. You must implement mechanisms that provide real-time data. The data must be looked at within a business context and this can only be done by clearly and defensibly linking exposures to financial impact. This all needs to be done by using standards – standard frameworks, standard models, and standard dashboards.

You need more than just a score to manage third party and supply chain risk.

ADVERTORIAL

Basel IV: Adapting to the new data requirements

Regnology

Anh Chu
Product Director
Regnology

The upcoming Basel IV changes have sent many organizations scrabbling as they prepare to address the vast implementation challenges on the horizon.

The primary challenge appears to be the scale of changes required across the entire Basel domain involving multiple risk teams. In isolation, each new requirement does not necessarily pose a huge implementation hurdle; but the task is significant when viewed holistically. The changes for operational risk's new standardization methodology require substantial data, more than previous obsolete calculation approaches. Organizations are now required to keep ten years of operational risk loss event data, which was not previously a requirement. On the market risk side, additional classification and guidance in place around FRTB and revisions to the Standardized Approach calculations by expanding sensitivity-based risk factors pose another hurdle. Credit risk has seen further refinement of asset classes and the introduction of some new ones never managed before, such as covered bonds. An increase in granularity also resulted, in some cases, increases in complexity for risk-weighted (RW) calculations, such as the introduction of managing Loan-To-Values (LTVs) for RW assignment. The removal of Internal Ratings-Based (IRB) as an approved approach for certain asset classes (i.e., large corporates) is another change under credit risk. Altogether, Basel IV have created a significant amount of data to be processed in a short amount of time. The inclusion of standardized floor calculations effectively doubling the number of calculations required at the same time period.

For global organizations, working with all the changes is a challenge not only due to the scale required in a short space of time, but also due to the added complexity when operating across jurisdictions. Financial institutions may find themselves subject to multiple interpretations, expectations, and deadlines. Each jurisdiction has its own interpretation, so organizations face a challenge when integrating and implementing, as variations or nuances can vary. In other cases, the requirements may be the same across jurisdictions but with differing and in some instances vary drastically timelines. Developing processes whilst being able to juggle different calculation methodologies, with some methodologies to be retired but in play in other jurisdictions. The variation in implementation timelines could provide an opportunity for organizations to leverage lessons learned from those on an earlier time scale.

Technology could play a vital role in implementing Basel IV standards and regulatory reporting. One such example is AI and how it could revolutionize the industry. It has great potential, although it has a long way to go. If organizations want to leverage AI technology, they will need to make certain investments needed, such as moving towards the cloud, ensuring the organization has a scalable infrastructure and a proper data management and data lineage system to handle the volume of data required to support AI for meaningful results. It is important to start the work now if organizations wish to leverage the power in the future.

AI has a multitude of uses that are already being implemented. AI can comb through regulations, identify changes, highlight where disparities may arise across jurisdictions, and identify a delta. The future of AI in regulatory reporting is even more optimistic, with far broader applications having a larger impact on how one can do capital. For example, AI may be able to analyze and find ways to optimize RWA. AI can help identify areas of improvement in data quality or change in asset class mix. To take advantage of this, organizations will need to start making the technological changes mentioned above.

The future of regulation, including Basel, is moving towards a far more detailed data-driven program. The granularity of data required for reporting, in general, is becoming more stringent and detailed. The shift is much more towards granular, standardized data and away from templates. Regulators expect the level of data that allows them to do their own calculations, analysis, and reporting. As each iteration of regulation comes out, not just in Basel, regulators are asking for more and more data with increasingly needed granularity. An example of this is the ECB's IReF (Integrated Reporting Framework) initiative. This is the future, the move by regulators increasing the level of granular data.

A WORD FROM THE INDUSTRY...

What are the key non-financial risks to look out for going into 2024?

Simon Cartlidge, *CRO*, Legal & General Retail Retirement Solutions

*"Heading into 2024, risk professionals need to remain vigilant to navigate an increasingly complex world safely (I say this every year). **Artificial Intelligence (AI)** presents myriad opportunities and threats, requiring an informed understanding and proportionate response. The financial services industry faces challenges in delivering **operational resilience** in line with regulatory expectations, influencing our oversight of key suppliers and putting a strain on these relationships. Embedding the **Consumer Duty** will see further evolution of metrics demonstrating the delivery of good outcomes and 'value' for customers. Finally, delivering effective **control over key projects** and the wider change portfolio will require careful management."*

Stephen Griffith, *Head of NFR / Operational Risk*, Bank of Ireland

*"Maintaining significant investment in cyber security remains critical, with new threats a constant. The evolution of **technology** and **data** management brings opportunities and risks, creating **disruption**. The industry must be alert to where machine learning and other areas of artificial intelligence are heading. The fast pace of **change** and multiple external factors create fraud, **people risks**, and potential capability gaps. Strong oversight of third parties and often complex supply chains continues to be essential. Firms must continue to raise standards through 2024, delivering against key regulations (Consumer Duty / Operational Resilience) whilst ensuring **good conduct, customer outcomes, and resilience.**"*

Freek van Velsen, *Partner*, CPI Risk Finance Governance

"I don't expect a major shift in key non-financial risks in 2024. Cyber risk will remain a key risk and might even get more important due to the increasing digitalization of processes and geopolitical tensions. Climate risk could attract more attention, where the opinion of the public can have a disruptive impact on current business practices. Next to this, CSRD reporting requirements will require companies to improve data quality and controls over non-financial reporting. Most companies at this time don't yet understand the requirements and the impact it will have on their business."

Sonia Jarvis, *Director, Quantitative Modeling*, Fannie Mae

"The industry has moved away from many sources of human-based risks; however, increased reliance on automated systems, out-of-the-box analytics, and assistive technologies has cultivated a culture of blind faith and misplaced trust. Overreliance on such tools, combined with a general lack of understanding of vendor and technological capabilities, has resulted in unwarranted complacency and unexpected risk exposures. Moving into 2024 we should aim for interdisciplinary approaches instead of siloed evaluation of technological, operational, and model risk across financial and non-financial business processes; increase due diligence and proactively educate all lines of defense - focus on estimating exposure rather than controlling the unpredictable."

Hugo Ramirez, *SVP Audit Responsible for Governance, Operational Risk & TPRM* , BBVA US Operations

"1. Effects of the expansion of the BRICS in the global economy and the geopolitical field.
2. The imminent take-off of the global economic recession.
3. Uncertainty will continue regarding the global economic/financial impact of the increased ESG focus.
4. The risk of cyber attacks will live with us for years to come; their increasing frequency, severity, and sophistication will have to be discussed.
5. Talent shortages and recruitment difficulties will also be risky in 2024 due to early retirement (a sequel to COVID-19) and the shortage and aging of the labor force.
6. Finally, the use of outsourcing will continue to worry companies and regulators next year."

Data-driven subledger tools are key to modern finance & risk management

Theresa Meawad
Head of Solutions Consulting
EVOLV SS&C Technologies

As the world continues to change rapidly and unexpectedly, banks are also transforming, particularly in addressing client needs for new loan offerings and creative modification options, while facing greater scrutiny from a focus on ESG (environmental, social and governance) issues. On top of this, banks are confronting new competition from FinTech firms that are agile, efficient, and subject to less regulatory pressure, which leaves traditional financial institutions seeking new ways to be profitable, to attract customers, and to create value for borrowers and depositors. Institutions need to bring together information from disparate parts of the organization in order to create actionable insights and strategies to address the demands and meet the challenges they face.

Meeting these demands has led to a push for better data to drive better decisions, putting finance and risk organizations squarely in the center of these conversations as the end point of an organization's data. Armed with the right tools, a modern finance organization can harness the power of its data to affect positive change. To aid in these transformations, many third-party subledgers have come to market to help these departments consolidate data and create insightful reporting. While these industry-agnostic, pre-built subledgers may be sufficient for many industries, they typically are not enough for banking institutions. Banks are more complex and demand fundamentally different reporting; a purpose-built subledger with world-class business intelligence tools can be transformative.

Part of what makes banks unique is the complexity of the main products they offer. Loans are challenging because each is individualized, illiquid and distinctive, and their accounting and valuation is specialized. Banks need a system that can consolidate data from various servicer and sub-servicer systems; make adjustments for GAAP accounting that can allow for a true view of interest income; provide intelligence into the risk and allowance process; and integrate with data from the credit department so that they can really understand all the risks and rewards associated with each loan, sub-portfolio and portfolio.

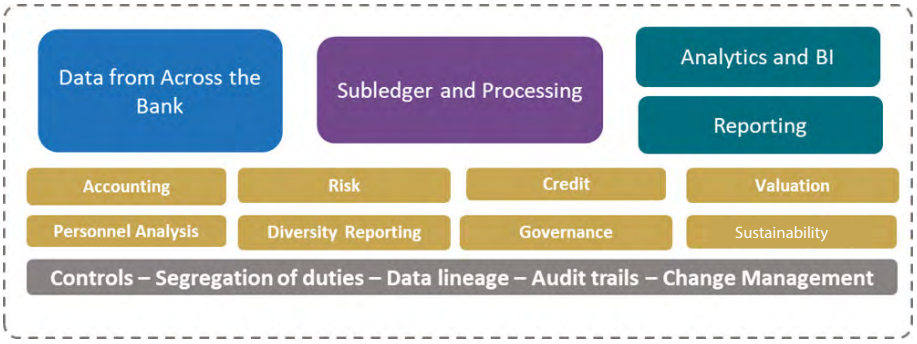
A purpose-built, modern loan subledger can bring together key information (i.e., personnel information, borrower information, and branch organization information) from various parts of the bank and combine it with purpose-built business intelligence tools that can make the collected information fundamentally understandable and shareable, and therefore reportable and actionable.

In addition, these bank-intelligent subledgers can help banks understand and report on key aspects of the business, such as:

- Branch performance, online performance, and other key performance indicators
- Sustainability impact of these loans on a variety of parameters, including ESG, as well as risks and impacts they may face, now or in the future
- Diversity reporting and impact on underserved populations, including yield analysis of the types of loans across various subpopulations, the effectiveness of each offering, and the outcomes' strategic alignment
- Governance reporting to review items that are specific to various individuals and roles, and better manage business risk in a controlled manner

By bringing together all the relevant information in one place, the right subledger can provide management a fuller understanding of a bank's performance and the drivers of its performance. In addition, these business intelligence tools can help banks take a deeper dive into emerging issues and allow all parts of the organization to be in sync and part of a unified front making progress towards its strategic vision and goals.

EVOLV Subledger Core Capabilities



SS&C EVOLV is extensible and highly configurable platform purpose built to solve the accounting, credit, regulatory, and reporting challenges for banks. To learn more about how SS&C EVOLV's integrated risk and finance functions can provide your institution with domain-aware insights, visit ssctech.com/products/evolv.

EVENTS CALENDAR 2023

Discover our wide range of premier risk and technology events across Europe and North America.

US Events

www.cefpro.com/digital-banking-usa

www.cefpro.com/climate-risk-usa

www.cefpro.com/oprisk-usa

www.cefpro.com/bsm-usa

www.cefpro.com/supply-chain

For more information, including agenda, speakers, location, and registration, visit www.cefpro.com/forthcoming-events

EMEA Events

www.cefpro.com/fraud-europe

www.cefpro.com/bsm-europe

www.cefpro.com/customer-experience

www.cefpro.com/climate-stress-testing

For more information, including agenda, speakers, location, and registration, visit www.cefpro.com/forthcoming-events